

3.1 Delta Training





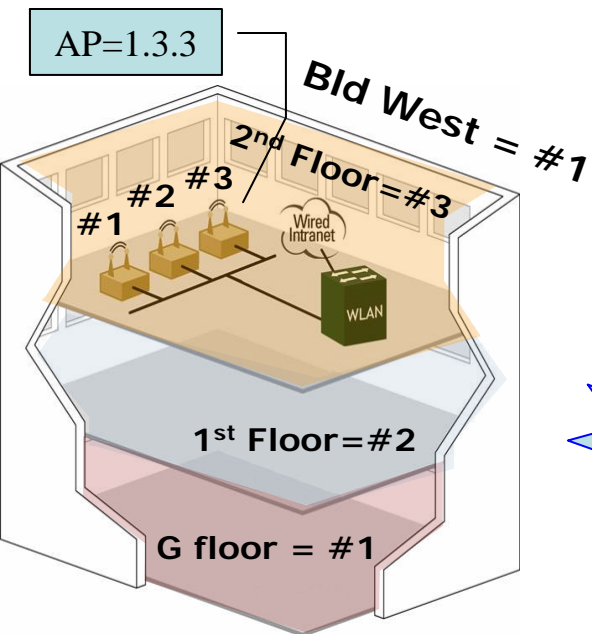
What's new in 3.1?

- AP Name/AP Group
- Profiles
- Licensing changes
- RF Plan FQLN and location
- ARM Enhancements
- Firewall Enhancements
- Authentication and Encryption
- Guest Provisioning Enhancements
- Master-Local IPSec
- Mobility Enhancements
- IDS Enhancements
- Troubleshooting and Management

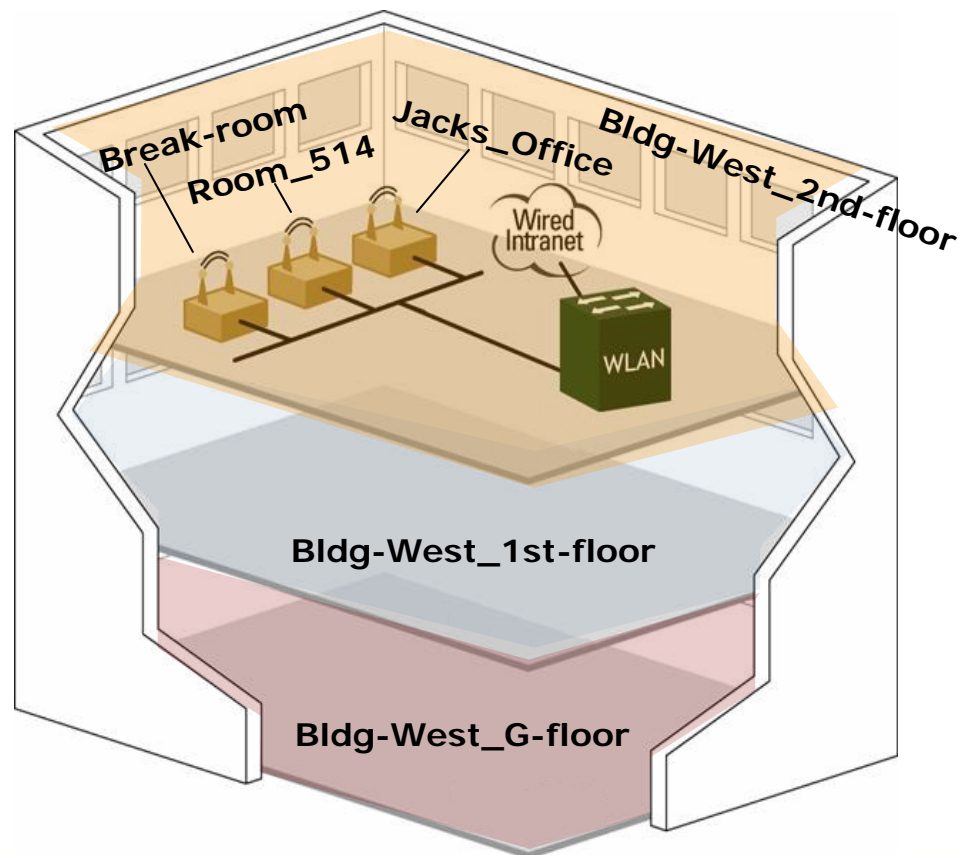
AP Names & AP Groups

No more B.F.N

- AP Config:
 - AP's now have a single GROUP
 - AP's now have a single NAME
- Both are alphanumeric text strings- you name them however it makes sense for your network



B.F.N Notation





The Advantage Of AP-Groups

Group the APs by logical function, not by floors



1. Define your services-
 - Employee WPA/2
 - Guest Access
2. Apply them where and when you want-
 - Employee Coverage Everywhere
 - Guest Access in Conference Rooms
 - Guest access in Reception from 9:00 – 17:00

- APs are now grouped, however you like- not just by floor e.g.
 - Cubicles
 - Conference Rooms
 - Reception
 - Open Space



AP Name/AP Group

- AP Name and AP Group are used to determine what configuration parameters/profiles are pushed to an AP
- AP Name must be unique
- If AP Name not set, then AP Wired MAC is used as AP Name
- AP may belong to one and only one group
- Create as many groups as needed, each with unique profile sets

Profiles & WebUI Navigation



ARUBATM
The **Mobile Edge** Company

Web UI Navigation

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Licenses will expire in 26 days Logout

Network

Network Summary

All WLAN Controllers
All Access Points
All Air Monitors
All Wired Access Points
Global Events

Controller

Controller Summary
Access Points
Wired Access Points
Wired Mux Ports
Air Monitors

Clients
Blacklist Clients

Firewall Hits

Ports

Inventory

Local Events

WLAN

<No SSIDs Found>

Voice

Voice Status
Call Density Report
Call Detail Report
Call Performance Report
Voice Clients
Voice Access Points

Debug

Network Summary

WLAN Network Status

	Total	Total	IPSEC	IPSEC
	Up	Down	Up	Down
WLAN Controllers	2	0		
Access Points	0	0	0	0
Air Monitors	0	1	0	0
Wired Access Points	0	0	0	0
Unprovisioned Access Points	1			
Duplicate AP Name	0			
RADIUS Servers	0	0		
LDAP Servers	0	0		

WLAN Performance Summary

	Last 5 Min	Last Hour	All
Load Balancing Events	0	0	0
Interference Events	0	0	0
Bandwidth Exceeded	0	0	0
Error Threshold Exceeded	0	0	0

Security Summary

WLAN Attack Summary

	Last 5 Min	Last Hour	All
Denial of Service Attacks	0	0	0
Impersonation Attacks	0	0	0
Signature Pattern Matches	0	0	0
Policy Violations	0	0	0
Unauthorized Devices Detected	0	0	0

Rogue AP Classification Summary

	Last 5 Min	Last Hour	All
Rogue APs Detected	0	0	0
Rogue APs Disabled	0	0	0
Suspected Rogue APs	0	0	0
Interfering APs Detected	0	0	0
Known Interfering APs	0	0	0

Client Classification Summary

	Last 5 Min	Last Hour	All
Valid Clients	0	0	0
Interfering Clients	0	0	0
Disabled Rogue Clients	0	0	0

WebUI Navigation

Monitoring

Configuration

Diagnostics

Maintenance

Plan

Events

Reports

Licenses will expire in 26 days

Save Configuration

Logout

Network

Controller

VLANs

Ports

IP

Security

Authentication

Access Control

Wireless

AP Configuration

AP Installation

Management

General

Administration

Certificates

SNMP

Logging

Clock

Advanced Services

Redundancy

IP Mobility

Stateful Firewall

VPN Services

Wired Access

Wireless

All Profiles

Network > Controller > System Settings

System SettingsLicenses

Controller Role

Master

Master IP Address

10.1.19.100

IPSec Key (IKE PSK)

Retype IPSec Key (IKE PSK)

Local Controller IPSec Keys

Local Controller IP Address	Key	Actions	
0.0.0.0	*****	Edit	Delete
<div>New</div>			

Loopback Interface

MAC Address

00:0B:86:51:04:E0

IP Address

10.1.19.100

Controller IP Details (Loopback)

MAC Address

00:0B:86:51:04:E0

IP Address

10.1.19.100

Subnet Mask

255.255.255.255

Spanning Tree Configuration

Spanning Tree Enabled

☒ Yes ☐ No

Forward Time

Hello Time

Max Age

Priority

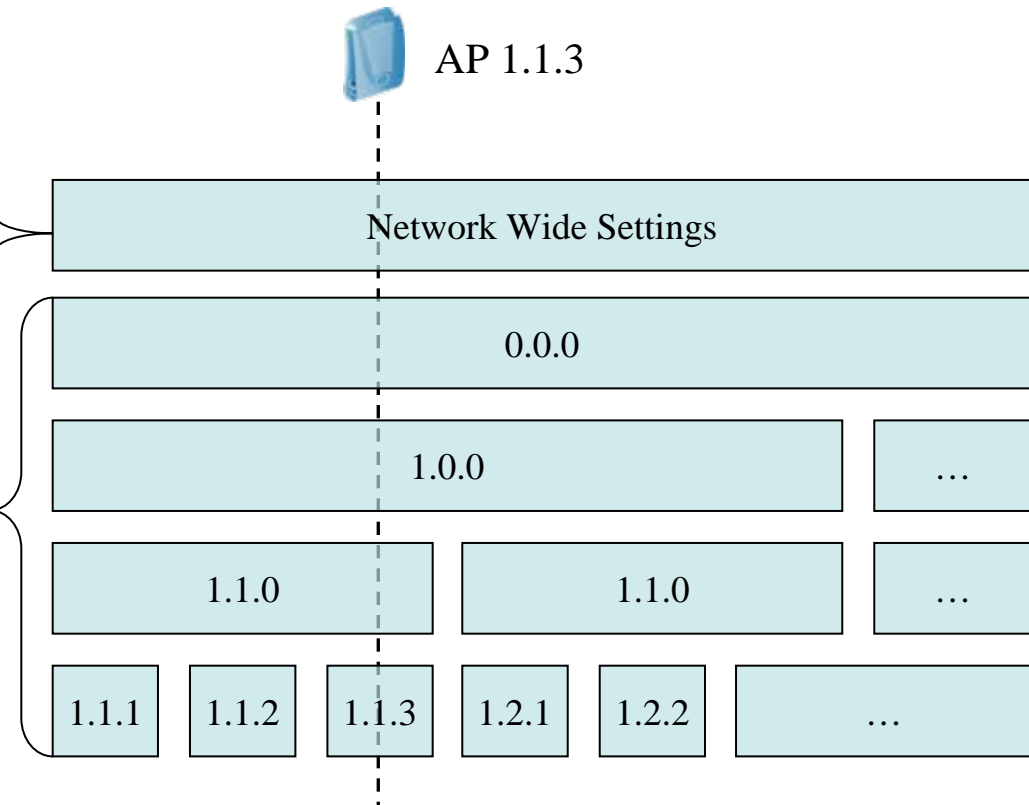
- Profiles are a powerful tool that allow administrators increased flexibility over other configuration methods
- All aspects of the configuration have been abstracted into profiles which are then applied to individual APs or (more commonly) to AP Groups

Configuration Prior to 3.x

- In AOS <3.x, the services over the air from an AP was determined by 2 major groups of settings-

- Network wide settings such as IDS, fast-roaming, mobility, XML API, derivation rules, auth-server, AAA Fastconnect, bandwidth contracts
- AP location settings such as ESSID, opmode, channel, ARM, tx-rates, voip-cac, static keys, Virtual-APs

- Virtual-APs were an add-on that lets you support multiple BSSIDs, with limited configuration that varies per release

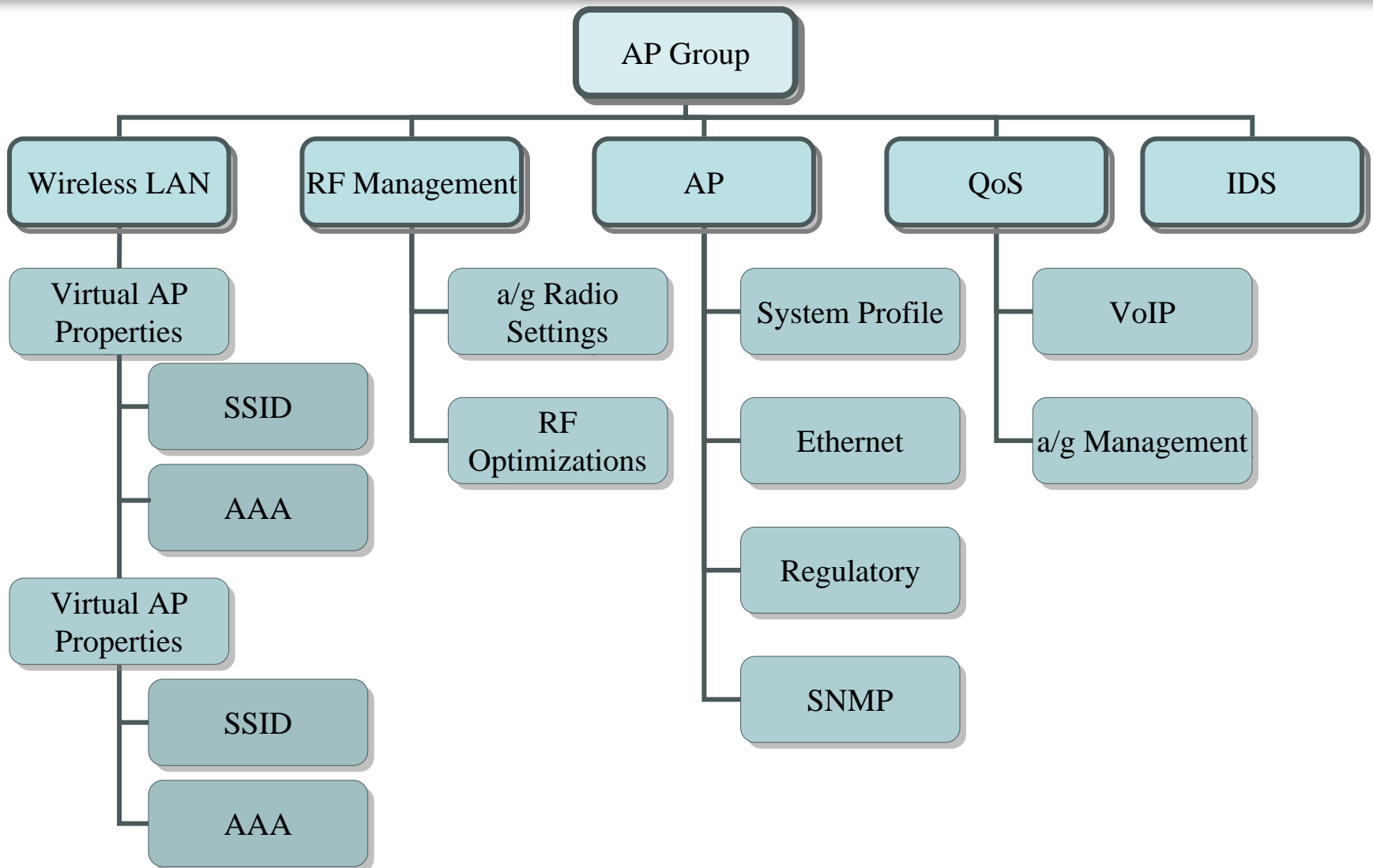




Profile Power

- 2.x could only have most settings network-wide:
 - `aaa dot1x auth-server foo1`
 - Sets the 802.1x auth server for the *entire network*
 - `wms assoc-rate-threshold 15`
 - Sets the IDS rate threshold for association frames for the *entire network*
- Profiles let you re-use settings for ease of maintenance:
 - Define a campus wide server-group for authentication and apply it to all chemistry & engineering & arts groups
 - The rest of the settings can be defined as new or previously existing profiles, but to add a new authentication server for everybody, you now can update only your one server group
- Virtual APs are now indistinguishable from the real AP
 - Most Parameters are now independent
 - EVERYTHING is now per Virtual-AP (eg. basic-rates, tx-rates, fast-roaming, mobility, XML API, derivation rules, Mac-auth, AAA Fastconnect, OKC, bandwidth contracts, etc)
 - Enable/disable each virtual-ap at will
 - Each virtual AP has its own initial role (no longer forced to use logon) and captive portal parameters are configured per-role

AP Groups and Profile



Profiles (cont.)

Monitoring Configuration Diagnostics Maintenance Plan Events Reports

Network
Controller
VLANs
Ports
IP

Security
Authentication
Access Control

Wireless
AP Configuration
AP Installation

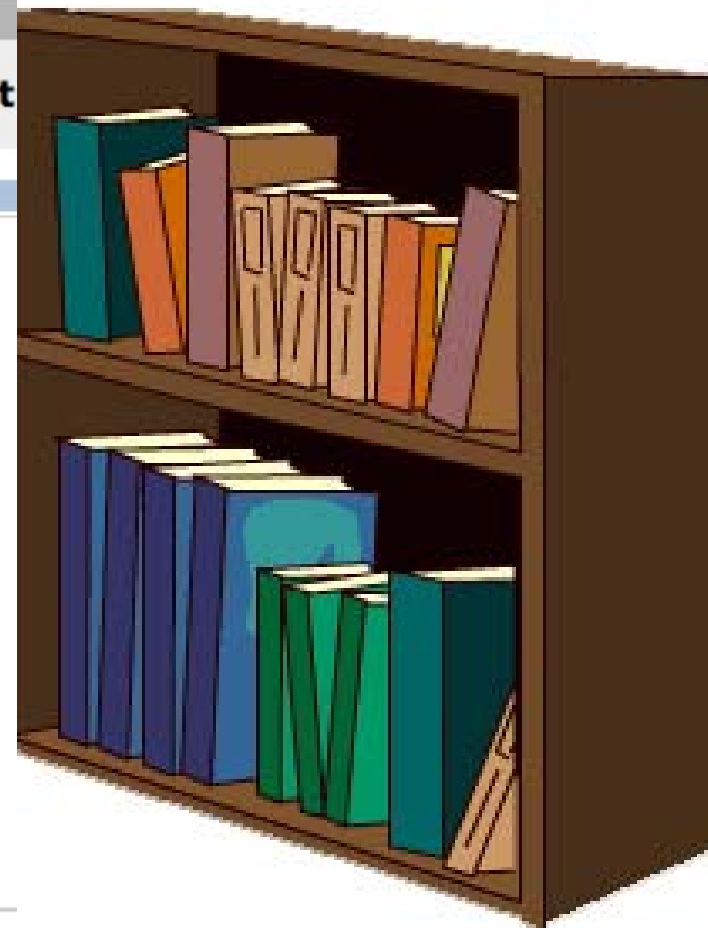
Management
General
Administration
Certificates
SNMP
Logging
Clock

Advanced Services
Redundancy
IP Mobility
Wired Access
Wireless

All Profiles

Advanced Services > All Profile Management

Profiles
<input checked="" type="checkbox"/> AP
<input checked="" type="checkbox"/> RF Management
<input checked="" type="checkbox"/> Wireless LAN
<input checked="" type="checkbox"/> SSID Profile
<input checked="" type="checkbox"/> Virtual AP profile
<input checked="" type="checkbox"/> default
<input checked="" type="checkbox"/> EMEA-Corp-Employee-VAP
<input checked="" type="checkbox"/> SSID Profile Employee-SSID
<input checked="" type="checkbox"/> AAA Profile EMEA-Employee-AAA
<input checked="" type="checkbox"/> US-Corp-Employee-VAP
<input checked="" type="checkbox"/> SSID Profile Employee-SSID
<input checked="" type="checkbox"/> AAA Profile US-Employee-AAA
<input checked="" type="checkbox"/> AAA Profile



Apply Profiles to AP Group

Monitoring

Configuration

Diagnostics

Maintenance

Plan

Events

Reports

Save Configuration

Log

Network

Controller

VLANs

Ports

IP

Security

Authentication

Access Control

Wireless

AP Configuration

AP Installation

Management

General

Administration

Certificates

SNMP

Logging

Clock

Advanced Services

Redundancy

IP Mobility

Wired Access

Wireless

All Profiles

Configuration > AP Group > Edit "US Building 2"

Profiles	Profile Details																												
<div><div>Wireless LAN</div><div>Virtual AP</div><div><div>US-Corp-Employee-VAP</div><div>SSID Profile Employee-SSID</div><div>AAA Profile US-Employee-AAA</div></div><div>US-Guest-VAP</div><div>SSID Profile Guest-SSID</div><div>AAA Profile US-Guest-AAA</div><div>RF Management</div><div>AP</div><div>QOS</div><div>IDS</div></div>	<div>Virtual AP > US-Corp-Employee-VAP</div> <div>Save As</div> <table><tbody><tr><td>Virtual AP enable</td><td><input checked="" type="checkbox"/></td><td>Allowed band</td><td>all</td></tr><tr><td>VLAN</td><td>109</td><td>Forward mode</td><td>tunnel</td></tr><tr><td>Deny time range</td><td>--NONE--</td><td>Mobile IP</td><td><input checked="" type="checkbox"/></td></tr><tr><td>DoS Prevention</td><td><input type="checkbox"/></td><td>Station Blacklisting</td><td><input checked="" type="checkbox"/></td></tr><tr><td>Blacklist Time</td><td>3600 sec</td><td>Authentication Failure Blacklist Time</td><td>3600</td></tr><tr><td>Fast Roaming</td><td><input type="checkbox"/></td><td>Strict Compliance</td><td><input type="checkbox"/></td></tr><tr><td>VLAN Mobility</td><td><input type="checkbox"/></td><td></td><td></td></tr></tbody></table> <div>Apply</div>	Virtual AP enable	<input checked="" type="checkbox"/>	Allowed band	all	VLAN	109	Forward mode	tunnel	Deny time range	--NONE--	Mobile IP	<input checked="" type="checkbox"/>	DoS Prevention	<input type="checkbox"/>	Station Blacklisting	<input checked="" type="checkbox"/>	Blacklist Time	3600 sec	Authentication Failure Blacklist Time	3600	Fast Roaming	<input type="checkbox"/>	Strict Compliance	<input type="checkbox"/>	VLAN Mobility	<input type="checkbox"/>		
Virtual AP enable	<input checked="" type="checkbox"/>	Allowed band	all																										
VLAN	109	Forward mode	tunnel																										
Deny time range	--NONE--	Mobile IP	<input checked="" type="checkbox"/>																										
DoS Prevention	<input type="checkbox"/>	Station Blacklisting	<input checked="" type="checkbox"/>																										
Blacklist Time	3600 sec	Authentication Failure Blacklist Time	3600																										
Fast Roaming	<input type="checkbox"/>	Strict Compliance	<input type="checkbox"/>																										
VLAN Mobility	<input type="checkbox"/>																												



Configuration - Summary

- What does it all fundamentally mean?
 - Per SSID/Group Enable/disable auth method
 - TKIP & AES/ WPA & WPA2 any mix, any SSID, any where
 - Per role (thus SSID/Group) Captive Portal
 - Per SSID/Group AAA Fastconnect
 - Per Group RF Monitoring & IDS
 - Arbitrary partitioning of Wireless Services to SSIDs and/or Areas

Licensing Changes



ARUBATM
The **Mobile Edge** Company



Licensing changes

- 3.1 adds a new “Voice Services” license.
- This license adds many new voice-specific features
- Voice-aware ARM scanning now requires the Voice license

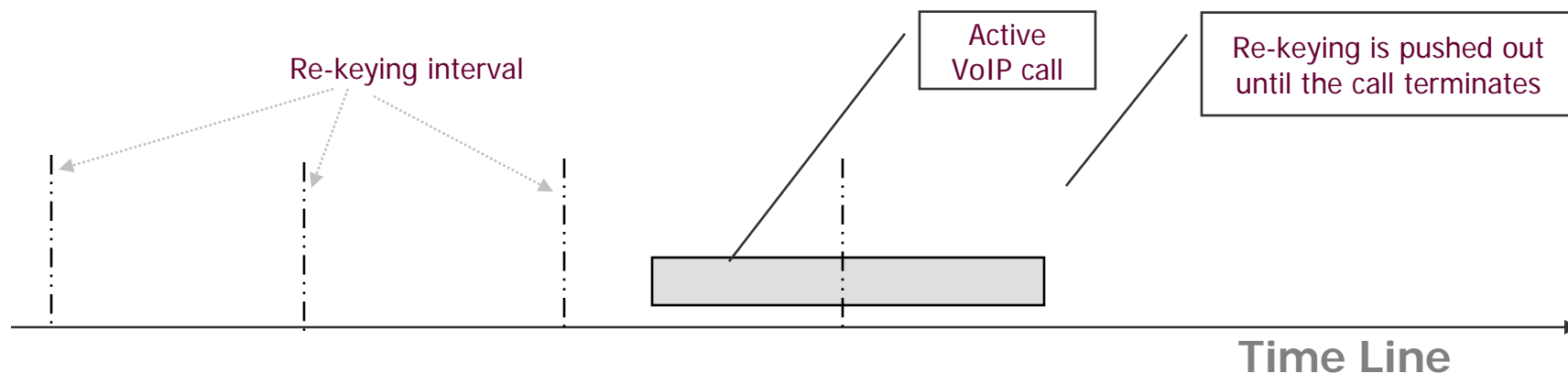


New Voice Features

- QoS
 - WMM
 - TSpec/TCLAS
 - UAPSD
 - Bandwidth contracts
 - Traffic Aware ARM scanning
 - TSpec/ TCLAS signalling enforcement
 - WMM voice queue content enforcement
 - Configurable WMM EDCA queue parameters
- VoIP
 - Battery Saving features
 - Battery Boost
 - VoIP proxy-arp
 - NoE
 - Voice aware 802.1x
 - WPA Fast Handover support
 - VoIP Manager for SIP
 - CAC enforcement
 - CAC strict enforcement
 - SIP authentication tracking
 - Early media / SIP session mgmt
 - Intelligent Mobile IP HA assignment

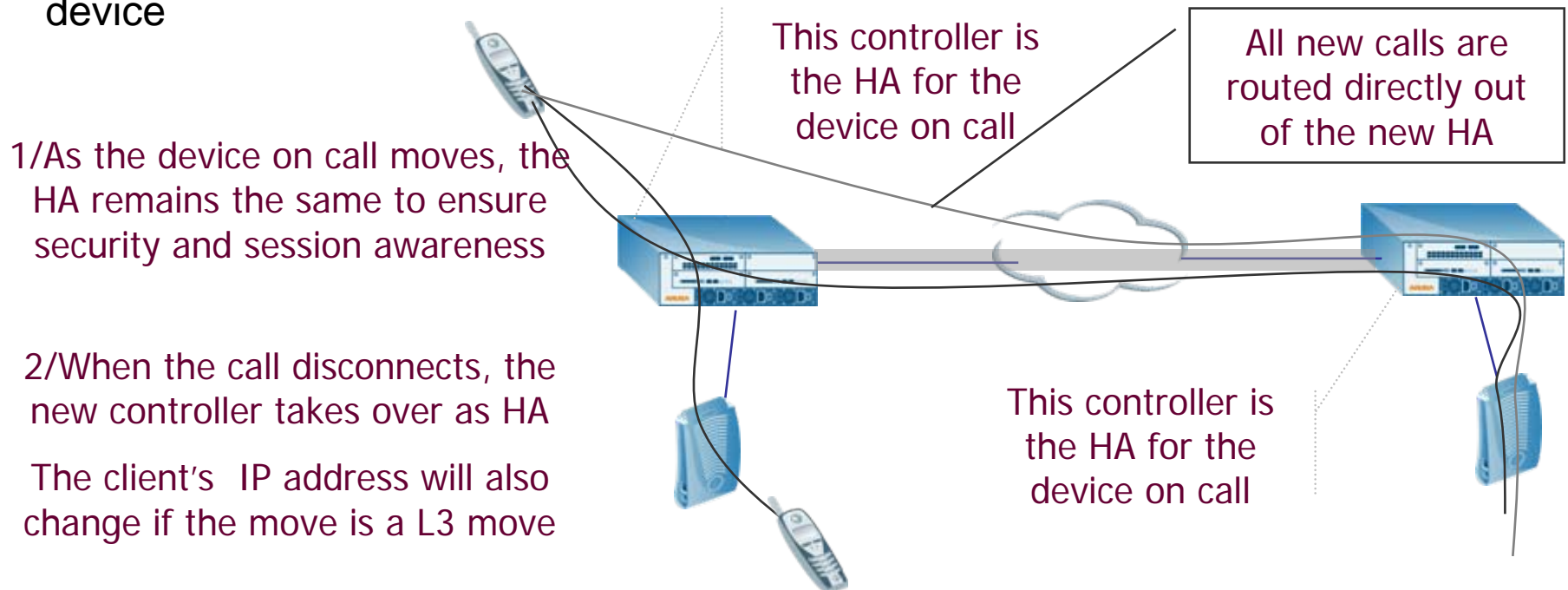
Voice Aware 802.1x / 802.11i

- 802.1x transactions can affect call quality when the device is on call. This feature allows the 802.1x transactions to be deferred till the end of call. The 4 way handshake will be postponed till after the call.
- 802.1x transactions will however occur when the client roams from one AP to another.
- The re-keying interval for the 802.11x profile can be modified to ensure that the rekey interval is longer for voice than it is for data.
- Feature not tied to Voice License



Voice Aware Mobility

- Voice Awareness is now also built into the Aruba Mobility algorithm.
- When a device on call moves from one controller to another, a tunnel is established across the 2 controllers with the traffic being tunneled back to the HA to ensure that the session awareness and security is not compromised by the move.
- Once the call is disconnected, the new controller takes over as the HA for the device





Battery Life features

- Battery Boost

- A wifi client in standby mode needs to wake up on regular interval to check for possible multicast frame. This regular interval was the DTIM setting. With this feature you can now move the DTIM to something very large (in the 100's range)

- Proxy Arp


- The MC v

- UAPSD (pa

- Saves battery while the phone is in a sleep state because phone can sleep between each voice packet

Standby battery life	Aruba 2.5.3	Aruba 3.x
Sanyo E02SA phone, clean environment	17 hours	100 hours

WEB UI Support

**Monitoring**

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Logout

Network
Network Summary
All WLAN Controllers
All Access Points
All Air Monitors
All Wired Access Points
Global Events
Controller
Controller Summary
Access Points
Wired Access Points
Wired Mux Ports
Air Monitors
Clients
Blacklist Clients
Firewall Hits
External Services Interface
Ports
Inventory
Local Events
WLAN
aruba-ap
aaa-ap
Voice
Voice Status
Call Density Report

Network Summary

WLAN Network Status

	Total Up	Total Down	IPSEC Up	IPSEC Down
WLAN Controllers	1	0		
Access Points	1	0	0	0
Air Monitors	0	0	0	0
Wired Access Points	0	0	0	0
Unprovisioned Access Points	0			
Duplicate AP Name	1			
RADIUS Servers	0	0		
LDAP Servers	0	0		

WLAN Performance Summary

	Last 5 Min	Last Hour	All
Load Balancing Events	0	0	0
Interference Events	0	0	0
Bandwidth Exceeded	0	0	0
Error Threshold Exceeded	0	0	0

Security Summary

WLAN Attack Summary

	Last 5 Min	Last Hour	All
Denial of Service Attacks	0	0	0
Man in the Middle Attacks	0	0	0
Signature Pattern Matches	0	0	0
Policy Violations	0	0	3

Rogue AP Classification Summary

	Last 5 Min	Last Hour	All
Rogue APs Detected	0	0	5
Rogue APs Disabled	0	0	0
Interfering APs Detected	17	194	397
Known Interfering APs	0	0	0

Client Classification Summary

	Last 5 Min	Last Hour	All
Valid Clients	0	0	0
Interfering Clients	1	13	16
Disabled Rogue Clients	0	0	0

Network

- Network Summary
- All WLAN Controllers
- All Access Points
- All Air Monitors
- All Wired Access Points
- Global Events

Controller

- Controller Summary
- Access Points
- Wired Access Points
- Wired Mux Ports

Air Monitors

- Clients
- Blacklist Clients
- Firewall Hits
- External Services Interface
- Ports
- Inventory
- Local Events

WLAN

- aruba-ap
- aaa-ap

Voice

- Voice Status
- Call Density Report
- Call Detail Report
- Call Performance Report
- Voice Clients
- Access Points Table

Debug

- Local Clients
- Process Logs

Custom Logs

<No Custom Logs Found>

Voice > Status

Active Calls

Graph

Protocol	Count
SIP	10
SCCP	2
SVP	5
Vocera	1

Rejected/Failed Calls

Graph

Reason	Count
Not Found (404)	1
Busy Here (486)	2
Service Unavailable (503)	1
Request Terminated (487)	4
Decline (603)	3
Unauthorized (401)	5
Address Incomplete (484)	7
Unsupported Media Type (415)	8
Temporary Unavailable (480)	6
Capacity Reached	4
Miscellaneous	9

APs

Graph

CAC State	Count
High Capacity Threshold	1
Call Handover Reservation Threshold	2
Load Balancing	1
OK	10

VoIP Clients

Graph

Client State	Count
Registered(Idle)	10
Registered(On-Call)	1
Unregistered	20

Call Quality

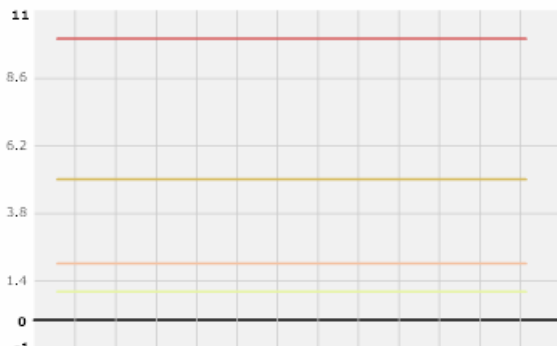
Graph

Band (R-Value)	Count
Red (<60)	1
Yellow (60-80)	2
Green (>80)	10

Statistics - Active Calls

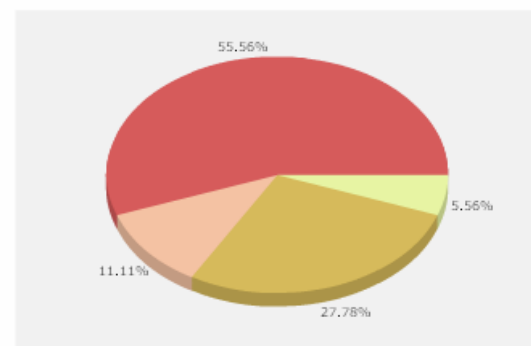
Line Graph

Macromedia Flash ActiveX control is required. You can download and install it from <http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,0,0>.



Pie Chart

Macromedia Flash ActiveX control is required. You can download and install it from <http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,0,0>.




Network

- Network Summary
- All WLAN Controllers
- All Access Points
- All Air Monitors
- All Wired Access Points
- Global Events

Controller

- Controller Summary
- Access Points
- Wired Access Points
- Wired Mux Ports
- Air Monitors
- Clients
- Blacklist Clients
- Firewall Hits
- External Services Interface
- Ports
- Inventory
- Local Events

WLAN

- aruba-ap
- aaa-ap

Voice

- Voice Status
- Call Density Report
- Call Detail Report**
- Call Performance Report
- Voice Clients
- Access Points Table

Debug

- Local Clients
- Process Logs

Custom Logs

<No Custom Logs Found>

Voice > Call Detail Report

 Report Type

Client Name	Orig Time	Dir	Number	Status	Dur	Reason	R-Value	Band
sip:1602	Oct 26 09:00:55	OG	To: sip:8690@10.100.117.101	CONNECTED	253		88.36	GREEN
sip:8690	Oct 26 09:00:55	IC	From: sip:1602@10.100.117.101	CONNECTED	253		93.36	GREEN
sip:1604	Oct 26 09:00:55	OG	To: sip:1605@10.100.117.101	SUCC	250		80.46	GREEN
sip:1605	Oct 26 09:00:55	IC	From: sip:1604@10.100.117.101	SUCC	250		90.6	GREEN

Statistics - Average Dur

Line Graph

Macromedia Flash ActiveX control is required. You can download and install it from <http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,0,0>.





Network

- Network Summary
- All WLAN Controllers
- All Access Points
- All Air Monitors
- All Wired Access Points
- Global Events

Controller

- Controller Summary
- Access Points
- Wired Access Points
- Wired Mux Ports
- Air Monitors
- Clients
- Blacklist Clients
- Firewall Hits
- External Services Interface
- Ports
- Inventory
- Local Events

WLAN

- aruba-ap
- aaa-ap

Voice

- Voice Status
- Call Density Report
- Call Detail Report

Call Performance Report

- Voice Clients
- Access Points Table

Debug

- Local Clients
- Process Logs

Custom Logs

<No Custom Logs Found>

Voice > Call Performance Report

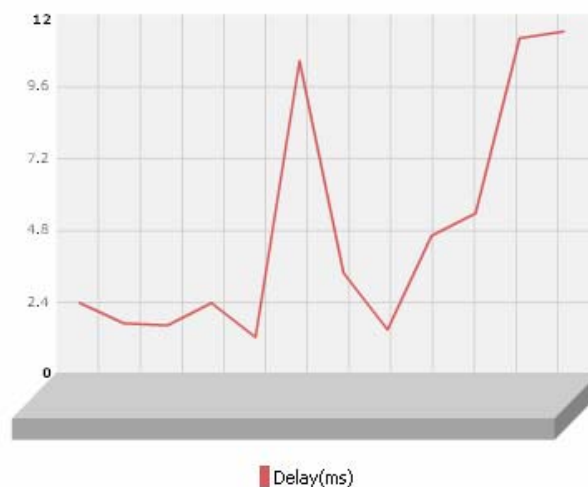
Report Type

Sample Time	Delay(ms)	AP-Switch Delay(ms)	Jitter	Packet Loss	R-Value	MOS	Band
Oct 26 09:00:00	11.45	0	1.91		0 95.45	4.77	GREEN
Oct 26 08:50:00	11.22	0	1.87		0 93.49	4.67	GREEN
Oct 26 08:40:00	5.36	0	0.89		0 94.63	4.73	GREEN
Oct 26 08:30:00	4.62	0	0.77		0 88.52	4.43	GREEN
Oct 26 08:20:00	1.48	0	0.25		0 62.36	3.12	YELLOW
Oct 26 08:10:00	3.37	0	0.56		0 78.09	3.9	YELLOW
Oct 26 08:00:00	10.45	0	1.01		0 90.45	4.52	GREEN
Oct 26 07:50:00	1.22	0	1.87		0 80.49	4.02	GREEN
Oct 26 07:40:00	2.36	0	1.89		0 84.63	4.23	GREEN
Oct 26 07:30:00	1.62	0	1.77		0 58.52	2.93	RED
Oct 26 07:20:00	1.68	0	1.25		0 62.36	3.12	YELLOW
Oct 26 07:10:00	2.37	0	0.36		0 78.09	3.9	YELLOW

Statistics - Delay(ms)

Line Graph

Macromedia Flash ActiveX control is required. You can download and install it from <http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,0,0>.



Voice > Client Troubleshooting

Client Summary

SIP Voice Client(s) Status

MAC	00:01:2a:01:ba:8d
IP Address	10.3.53.5
Call Status	Idle
Role	guest
Protocol	SIP
Server IP Address	10.100.117.101
Number of Handovers	3
Time Since Last Association(sec)	30

802.11 Status Table Entries

Client Name	sip:8690
Assoc State/Dur(sec)	Associated/50
Retry Count	2
PowerSave State	ON
Data Rate(Mbps)	0.7
TSPEC/TCLAS	

Roaming Status

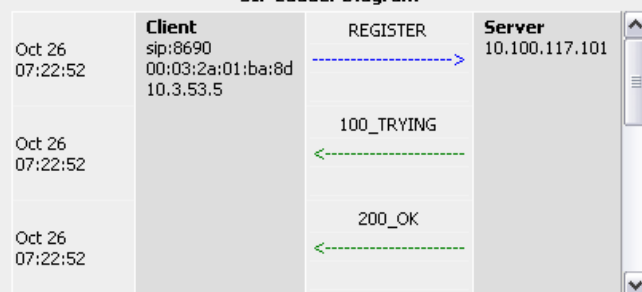
Time	To	From
Oct 26 07:22:52		ap2
Oct 26 07:28:04	ap2	ap1
Oct 26 07:29:50	ap1	ap2
Oct 26 07:30:40	ap2	ap1

Client Detail Report

Client Name	Orig Time	Dir	Number	Status	Dur	Reason	R-Value	Band	BSSID	ESSID	AP(IP Address)
sip:8690	Oct 26 09:00:55	IC	From: sip:1602@10.100.117.101	CONNECTED	253		93.36	GREEN	00:0b:86:c0:cc:06	s16wep	10.3.53.251

Signalling

SIP Ladder Diagram



Datapath Session Table Entries

Source IP	Destination IP	Prot	SPort	DPort	Cntr	Prio	ToS	Age	Destination	Flags
10.3.53.5	10.100.102.204	17	9001	15811	0	0	0	1	1/23	FY
10.3.53.5	10.100.102.204	17	9001	11299	0	0	0	1	1/23	FY
10.100.102.204	10.3.53.5	17	15811	9001	0	0	0	0	1/23	FC
10.100.102.204	10.3.53.5	17	11299	9001	0	0	0	0	1/23	FC

Flags: F - fast age, S - src NAT, N - dest NAT

D - deny, R - redirect, Y - no syn

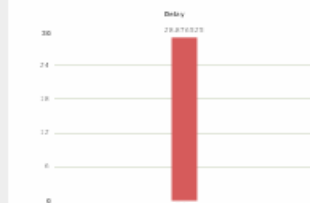
H - high prio, P - set prio, T - set ToS

C - client, M - mirror, V - VOIP

Media

Statistics - Call Quality Histogram

Histogram

Macromedia Flash ActiveX control is required. You can download and install it from [Here](#).Macromedia Flash ActiveX control is required. You can download and install it from [Here](#).Macromedia Flash ActiveX control is required. You can download and install it from [Here](#).Macromedia Flash ActiveX control is required. You can download and install it from [Here](#).

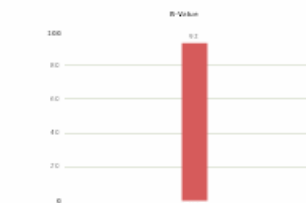
Delay



Jitter



Pkt Loss



R-Value



Voice Features: Voice scale and quality



Call Capacity

- T-Spec
- Strict accuracy



Quality of Service

- WMM
- WMM Enforcement



Handoffs

- Secure Handoff Performance

Battery Life

- U-APSD / WMM-PS
- Proxy ARP
- Battery Boost

RF Plan, FQLN, and ARM



ARUBATM

The **Mobile Edge** Company



RF Plan changes in 3.1

- FQLN
- Power level display changes
- .11a Channel updates
- ARM updates

- Use Fully Qualified Location Name (FQLN) to associate APs and AMs to a location
- FQLN Format:
APname.Floor.Building.Campus
- Used to map AP to Campus, Building, Floor in RF Plan
- AP Name and AP Group still used for assigning profiles

Setting FQLN

Monitoring Configuration Diagnostics Maintenance **Plan** Events Reports Licenses will expire

Plan > Campus List

Search Results [Search](#)

<input type="checkbox"/>	Name ▲	Buildings	Modified Time ▼
<input type="checkbox"/>	Home	1	10:25:41 11/14/2006
<input type="checkbox"/>	default	2	02:13:16 11/13/2006

1 | 1-2 of 2 10 ▼

New Campus Browse Campus... Delete Campuses Export Import... **AP FQLN Mapper...**

Select building and Mapper

Assign FQLN

Plan > AP FQLN Mapper

Search

Hide Search

AP Name	<input type="text"/>	FQLN	<input type="text"/>
Wired MAC	<input type="text"/>	Serial Number	<input type="text"/>
IP Address	<input type="text"/>	Status	Any <input type="button" value="v"/>

Number of results per page: 10

Search Result

Search

<input type="checkbox"/>	AP Name ▲	Wired MAC ▲	Serial # ▲	AP Type ▲	IP Address ▲	FQLN ▲	Status ▲	Last Update Time ▼
<input type="checkbox"/>	Home 61	00:0b:86:c2:d9:44	A30055648	61	192.168.2.230	Home 61.Floor 1.Home.default	up	11:52:21 11/17/2006
<input type="checkbox"/>	Home 70	00:0b:86:c4:d8:6a	A50028617	70	192.168.2.238	Home 70.Floor 1.Home.default	up	11:51:47 11/17/2006

1 | 1-2 of 2 10

Campus: Home Building: South Roanoke Floor: Floor 1

Dropdown options appear only after
Campus, Building and Floor have been created

Note: Setting FQLN reboots APs

- NOTE: you do not have to use the FQLN mapper if you simply set the AP Name in the AP Installation menu to be the same as the AP Name in RF Plan. The system will automatically configure the FQLN when the AP boots.



Power Level Adjustment

- Aruba radio power levels are adjustable between 0 and 4
 - 4 is highest
- Calibration will automatically set the power level to avoid interference with other APs
- Power levels will be dynamically adjusted to fill in holes if an AP fails



Channel Selection

- APs operate most efficiently when they are the only AP on the channel
- Calibration will automatically assign channels to each AP to minimize interference
- Only channels approved by the appropriate country regulations will be assigned
 - For example, in North America this is
 - 802.11b/g = 1, 6, and 11
 - 802.11a = 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165

ARM Settings

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Licenses will expire in 29 days Save Configuration Log

Network
Controller
VLANs
Ports
IP

Security
Authentication
Access Control

Wireless
AP Configuration
AP Installation

Management
General
Administration
Certificates
SNMP
Logging
Clock

Advanced Services
Redundancy
IP Mobility
Stateful Firewall
VPN Services
Wired Access

Configuration > AP Group > Edit "Building2"

Profiles	Profile Details																																				
<ul style="list-style-type: none">+ Wireless LAN- RF Management<ul style="list-style-type: none">- 802.11a radio profile defaultAdaptive Radio Management (ARM) Profile default+ 802.11g radio profile defaultRF Optimization profile defaultRF Event Thresholds profile default+ AP+ QOS+ IDS	<p>Adaptive Radio Management (ARM) Profile > Save As Reset</p> <p>default ▾</p> <table><tbody><tr><td>Assignment</td><td>single-band ▾</td><td>Client Aware</td><td><input checked="" type="checkbox"/></td></tr><tr><td>Max Tx Power</td><td>30 ▾</td><td>Min Tx Power</td><td>11 ▾</td></tr><tr><td>Multi Band Scan</td><td><input checked="" type="checkbox"/></td><td>Rogue AP Aware</td><td><input type="checkbox"/></td></tr><tr><td>Scan Interval</td><td>10 sec</td><td>Scanning</td><td><input checked="" type="checkbox"/></td></tr><tr><td>Scan Time</td><td>110 msec</td><td>VoIP Aware Scan</td><td><input type="checkbox"/></td></tr><tr><td>Power Save Aware Scan</td><td><input checked="" type="checkbox"/></td><td>Ideal Coverage Index</td><td>5</td></tr><tr><td>Acceptable Coverage Index</td><td>2</td><td>Wait Time</td><td>15 sec</td></tr><tr><td>Free Channel Index</td><td>25</td><td>Backoff Time</td><td>240 sec</td></tr><tr><td>Error Rate Threshold</td><td>50 %</td><td>Error Rate Wait Time</td><td>30 sec</td></tr></tbody></table> <p>Apply</p>	Assignment	single-band ▾	Client Aware	<input checked="" type="checkbox"/>	Max Tx Power	30 ▾	Min Tx Power	11 ▾	Multi Band Scan	<input checked="" type="checkbox"/>	Rogue AP Aware	<input type="checkbox"/>	Scan Interval	10 sec	Scanning	<input checked="" type="checkbox"/>	Scan Time	110 msec	VoIP Aware Scan	<input type="checkbox"/>	Power Save Aware Scan	<input checked="" type="checkbox"/>	Ideal Coverage Index	5	Acceptable Coverage Index	2	Wait Time	15 sec	Free Channel Index	25	Backoff Time	240 sec	Error Rate Threshold	50 %	Error Rate Wait Time	30 sec
Assignment	single-band ▾	Client Aware	<input checked="" type="checkbox"/>																																		
Max Tx Power	30 ▾	Min Tx Power	11 ▾																																		
Multi Band Scan	<input checked="" type="checkbox"/>	Rogue AP Aware	<input type="checkbox"/>																																		
Scan Interval	10 sec	Scanning	<input checked="" type="checkbox"/>																																		
Scan Time	110 msec	VoIP Aware Scan	<input type="checkbox"/>																																		
Power Save Aware Scan	<input checked="" type="checkbox"/>	Ideal Coverage Index	5																																		
Acceptable Coverage Index	2	Wait Time	15 sec																																		
Free Channel Index	25	Backoff Time	240 sec																																		
Error Rate Threshold	50 %	Error Rate Wait Time	30 sec																																		

Firewall Enhancements



ARUBATM
The **Mobile Edge** Company



Traffic-Aware ARM scanning

- Allows one to configure firewall rules that describe traffic types that should cause ARM to pause scanning on whatever AP the rule is triggered
- It can be used to support Voice, Video, or other delay-sensitive protocols for which we are not stateful (ie: not SIP, SVP, SCCP, Vocera).



Configuration

- Configuration examples

(config) # ip access-list session mycriticalapp

(config-sess) # any any udp <port> permit disable-scanning

(config-sess) # any any tcp <port> permit disable-scanning



Troubleshooting

- The best way to troubleshoot this feature is to look at the session table (“show datapath session table”) and verify that the VOIP flag is set for the specific session.
- (A800) (config) #show ap debug radio-stats ap-name AP70 radio 0 advanced | include Scan

Scan Requests 108593

Scan Rejects **305**

Scan Success 108288

ARM Scan Frames 4882960



Ethertype and MAC FW policies

- ArubaOS 3.1 now allows the addition of Ethertype and MAC ACLs to user roles
- Simply create an Ethertype or MAC ACL and apply it to a user role the same way as a session policy

Per-SSID Bandwidth Contracts

- Allocates “air time” to virtual APs on a given physical AP
- SSIDs may burst above configured limit as long as other SSIDs are not starved

Profile Details

802.11g Traffic Management profile >

--NEW--

test

Reset

Proportional BW Allocation	<div>25% 1.0.0-a</div> <div>15% 1.1.16-g_tags</div> <div>25% 1.1.14_guest-demo</div> <div>35% 1.1.39-a_alpha-xsec</div>	<div>Delete</div>	Report interval (minutes)	<div>5</div> min
	<div>Virtual AP</div> <div>1.0.0-a_alpha-a</div> <div>Share(%) 0</div> <div>Add</div>			

Authentication and Encryption



ARUBATM

The **Mobile Edge** Company



Module Overview

- Authentication
 - SSID
 - MAC
 - Captive Portal
 - VPN
 - 802.1x
- Encryption
 - Layer 2 vs. Layer 3
- Wireless security protocols
 - WPA
 - 802.11i/WPA 2.0

Authentication



ARUBATM
The **Mobile Edge** Company



SSID Authentication

- A user can be authenticated simply by associating with a given SSID
- A policy is created such that anyone associating with a given SSID is granted certain permissions
- Weak encryption offerings (WEP), and high administrative overhead (creating a separate SSID for each user group) make SSID a poor choice

SSID Authentication Configuration

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Licenses will expire in 23 days Save Configuration Log

Network
Controller
VLANs
Ports
IP

Security
Authentication
Access Control

Wireless
AP Configuration
AP Installation

Management
General
Administration
Certificates
SNMP
Logging
Clock

Advanced Services
Redundancy
IP Mobility
Stateful Firewall
VPN Services
Wired Access

Configuration > AP Group > Edit "Building2"

Profiles		Profile Details	
<input type="checkbox"/> Wireless LAN		AAA Profile > EMEA-Corp Save As Reset	
<input type="checkbox"/> Virtual AP			
<input type="checkbox"/> T9-Corp-Building2			
<input checked="" type="checkbox"/> SSID Profile	T9-corp-Employee		
<input type="checkbox"/> AAA Profile	EMEA-Corp		
<input checked="" type="checkbox"/> RF Management			
<input checked="" type="checkbox"/> AP			
<input checked="" type="checkbox"/> QOS			
<input checked="" type="checkbox"/> IDS			

Initial role		MAC Authentication Default Role	
logon		guest	

802.1X Authentication Default Role		User derivation rules	
Employee		--NONE--	

Wired to Wireless Roaming		SIP authentication role	
<input checked="" type="checkbox"/>		--NONE--	

MAC Authentication Profile	
MAC Authentication Server Group	default
802.1X Authentication Profile	T9-Corp
802.1X Authentication Server Group	Campus
RADIUS Accounting Server Group	

Apply

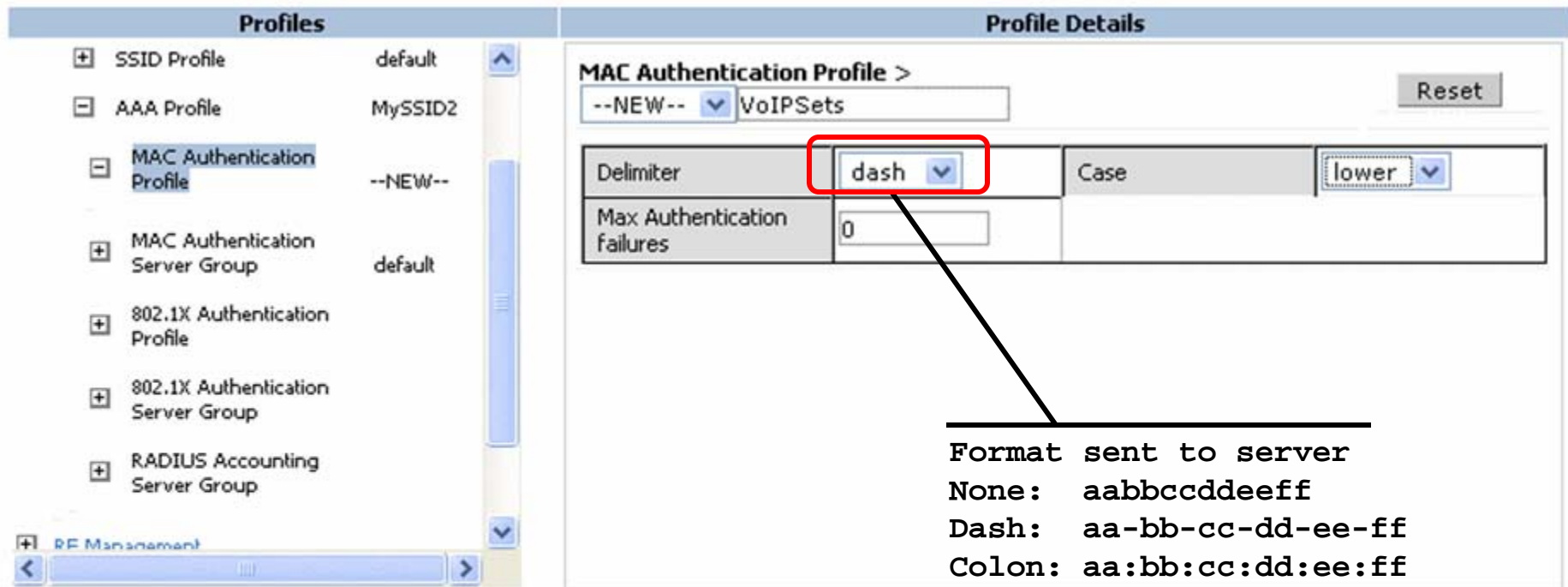


MAC Authentication

- A user's MAC address can be used to establish Identity
- However, MAC addresses can be spoofed by an attacker
- Useful for devices that cannot run authentication software (handheld scanners, printers, etc)

- There are 2 different mechanisms for performing MAC Authentication
 - MAC Auth Profile
 - User Derivation Rules

MAC Auth Profile



Profiles

- SSID Profile default
- AAA Profile MySSID2
- MAC Authentication Profile --NEW--**
- MAC Authentication Server Group default
- 802.1X Authentication Profile
- 802.1X Authentication Server Group
- RADIUS Accounting Server Group

Profile Details

MAC Authentication Profile >

--NEW-- VoIPSets Reset

Delimiter	dash	Case	lower
Max Authentication failures	0		

Format sent to server

None: aabbccddeeff

Dash: aa-bb-cc-dd-ee-ff

Colon: aa:bb:cc:dd:ee:ff

Commands

[Hide Commands](#)

```
aaa authentication mac "VoIPSets"  
  delimiter dash  
aaa profile "MySSID2"  
  authentication-mac "VoIPSets"
```

Specify Authentication Server

Profiles

- SSID Profile default
- AAA Profile MySSID2
- MAC Authentication Profile VoIPSets
- MAC Authentication Server Group default**
- 802.1X Authentication Profile
- 802.1X Authentication Server Group
- RADIUS Accounting Server Group

Profile Details

MAC Authentication Server Group > default [Save As] [Reset]

Servers

Name	trim-FQDN	match-FQDN	Server-Type	Actions
IAS	No		Radius	Delete ▲ ▼
Internal	No		Internal	Delete ▲ ▼

[New]

Server Rules

Priority	Attribute	Operation	Operand	Action	Value	Actions
1	role	value-of		set role		Delete ▲ ▼

[Apply] [Cancel] [Hide Commands]

Commands

User Derivation Rules

Monitoring

Configuration

Diagnostics

Maintenance

Plan

Events

Reports

Licenses will expire in 29 days

Save Configuration

Logout

Network

Controller

VLANs

Ports

IP

Security

Authentication

Access Control

Wireless

AP Configuration

AP Installation

Management

General

Administration

Certificates

SNMP

Logging

Clock

Advanced Services

Redundancy

IP Mobility

Stateful Firewall

VPN Services

Wired Access

Security > Authentication > User Rules

Servers

AAA Profiles

L2 Authentication

L3 Authentication

User Rules

Advanced

User Rules Summary

scangunOUI

Rules-set: scangunOUI

Priority	Attribute	Operation	Operand	Action	Value	Total Hit	New Hit	Actions
None found								

Add new rules

Set Type

Role

Rule Type

MAC Address

Condition

starts-with

Value

01:23:45

Roles

scanners

Add

Cancel

Apply

ARUBA™

The Mobile Edge Company

Confidential

©2005 All rights reserved

User Derivation Rules (cont.)

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Licenses will expire in 23 days Save Configuration Log

Network
Controller
VLANs
Ports
IP

Security
Authentication
Access Control

Wireless
AP Configuration
AP Installation

Management
General
Administration
Certificates
SNMP
Logging
Clock

Advanced Services
Redundancy
IP Mobility
Stateful Firewall
VPN Services
Wired Access

Configuration > AP Group > Edit "Building2"

Profiles		Profile Details	
<div>[-] Wireless LAN</div> <div>[-] Virtual AP</div> <div>[-] T9-Corp-Building2</div> <div> [+] SSID Profile T9-corp-Employee</div> <div> [-] AAA Profile EMEA-Corp</div> <div> [+] RF Management</div> <div> [+] AP</div> <div> [+] QOS</div> <div> [+] IDS</div>		AAA Profile > EMEA-Corp Save As Reset	
Initial role	logon	MAC Authentication Default Role	guest
802.1X Authentication Default Role	Employee	User derivation rules	--NONE--
Wired to Wireless Roaming	<input checked="" type="checkbox"/>	SIP authentication role	--NONE--
MAC Authentication Profile			
MAC Authentication Server Group		default	
802.1X Authentication Profile		T9-Corp	
802.1X Authentication Server Group		Campus	
RADIUS Accounting Server Group			

Apply



Internal Database

- Built into the controller
- Simple authentication option
- Can be used with EAP-offload

Internal Database (continued)

Monitoring

Configuration

Diagnostics

Maintenance

Plan

Events

Reports

Licenses will expire in 23 days

Save Configuration

Log

Network

Controller

VLANs

Ports

IP

Security

Authentication

Access Control

Wireless

AP Configuration

AP Installation

Management

General

Administration

Certificates

SNMP

Logging

Clock

Advanced Services

Redundancy

IP Mobility

Stateful Firewall

VPN Services

Wired Access

Security > Authentication > Servers

Servers

AAA Profiles

L2 Authentication

L3 Authentication

User Rules

Advanced

+ Server Group

+ RADIUS Server

+ LDAP Server

+ Internal DB

+ TACACS Server

Internal DB Maintenance

Maximum Expiration min

Export

Import

Delete All Users

Repair Database

Users

User Name	Password	Role	Contact Information	Enabled	Expiry	Action
<div>Add User</div>						

Apply



Captive Portal

- Web-based authentication method (SSL)
- Enabled by default
- Typically found in Public Hotspots, Universities
- User associates (open or static WEP), receives IP address.
- Launches web browser, forced to authentication web page
- May authenticate against internal or external server
- Can also be used with Sygate On Demand Agent (SODA) for client integrity
- After successful authentication, Role assigned



Captive Portal Configuration Steps

Step 1: Configure the auth-server (external or internal-db)

Step 2: Create a server group and assign the configured auth-server to it.

Step 3: Create a Captive Portal profile and configure the required parameters (default role, server group, etc.)

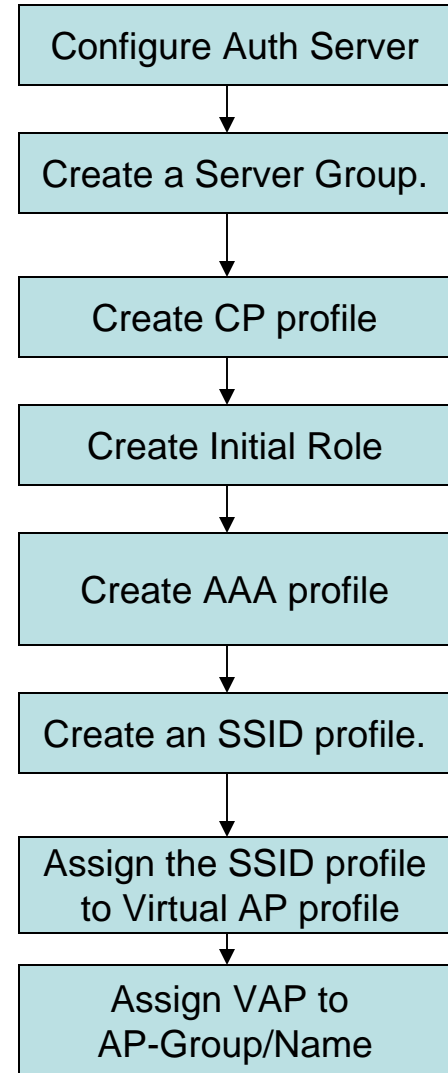
Step 4: Create an Initial Role and assign the Captive Portal profile

Step 5: Create a AAA profile and assign the Initial Role.

Step 6: Create an SSID profile and configure the required encryption (open), SSID name, and other parameters.

Step 7: Create a Virtual AP profile and assign the AAA and SSID profiles previously created to it.

Step 8: Assign the Virtual AP to an AP Group/AP Name.



Create Captive Portal Profile

Monitoring

Configuration

Diagnostics

Maintenance

Plan

Events

Reports

Licenses will expire in 29 days

Save Configuration

Logout

Network

Controller

VLANs

Ports

IP

Security

Authentication

Access Control

Wireless

AP Configuration

AP Installation

Management

General

Administration

Certificates

SNMP

Logging

Clock

Advanced Services

Redundancy

IP Mobility

Stateful Firewall

VPN Services

Wired Access

Wireless

Security > Authentication > L3 Authentication

Servers

AAA Profiles

L2 Authentication

L3 Authentication

User Rules

Advanced

Captive Portal Authentication Profile

Acme-CP-profile

Server Group Internal

default

VPN Authentication Profile

Captive Portal Authentication Profile > Acme-CP-profile

Save AsReset

Default Role	guest	Redirect Pause	10 sec
User Login	<input checked="" type="checkbox"/>	Guest Login	<input type="checkbox"/>
Logout popup window	<input checked="" type="checkbox"/>	Use HTTP for authentication	<input type="checkbox"/>
Logon wait minimum wait	5 sec	Logon wait maximum wait	10 sec
logon wait CPU utilization threshold	60 %	Max Authentication failures	0
Show FQDN	<input type="checkbox"/>	Use CHAP (non-standard)	<input type="checkbox"/>
Sygate-on-demand-agent	<input type="checkbox"/>	Login page	/auth/index.html
Welcome page	/auth/welcome.html	Show Welcome Page	<input checked="" type="checkbox"/>
Proxy Server			

Commands

Apply

View Commands



Captive Portal Login

Portal Login

https://securelogin.arubanetworks.com/auth/index.html?host=172.16.0.254&url=/&s Google

Google AMASuperbike.com /. ORI Utilities Aruba Directory Iris

REGISTERED USER

USERNAME

PASSWORD

Log In

GUEST USER

EMAIL

Log In

Logging in as a guest user indicates you have read and accepted the [Acceptable Use Policy](#).

ARUBA

AF The Mobil

Assign CP Profile to Initial Role

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Licenses will expire in 29 days Save Configuration Logout

Network
Controller
VLANs
Ports
IP

Security
Authentication
Access Control

Wireless
AP Configuration
AP Installation

Management
General
Administration
Certificates

Security > User Roles > Edit Role(guest-login)

User Roles System Roles Policies Time Ranges Guest Access

« Back

Firewall Policies

Name	Rule Count	AP Group	Action
captiveportal	3		Edit Delete ▲ ▼
Guest-Logon-Access	4		Edit Delete ▲ ▼
Add			

Captive Portal Profile

Acme-CP-profile

Acme-CP-profile ▼

[Change](#)

[Apply](#)

Commands

```
user-role "guest-login"
captive-portal "Acme-CP-profile"
!
```

[Hide Commands](#)

Define Initial Role in AAA Profile

Monitoring

Configuration

Diagnostics

Maintenance

Plan

Events

Reports

Licenses will expire in 30 days

Save Configuration

Log

Network

Controller

VLANs

Ports

IP

Security

Authentication

Access Control

Wireless

AP Configuration

AP Installation

Management

General

Administration

Certificates

SNMP

Logging

Clock

Advanced Services

Redundancy

IP Mobility

Stateful Firewall

External Services

Wired Access

Wireless

All Profiles

Advanced Services > All Profile Management

Profiles

Wireless LAN

SSID Profile

Virtual AP profile

AAA Profile

default

default-dot1x

default-dot1x-psk

default-mac-auth

default-open

EMEA-Employee-AAA

US-Employee-AAA

US-Guest-AAA

Profile Details

AAA Profile > US-Guest-AAA

Save As

Reset

Initial role	guest-login	MAC Authentication Default Role	guest
802.1X Authentication Default Role	guest	User derivation rules	--NONE--
Wired to Wireless Roaming	<input checked="" type="checkbox"/>	SIP authentication role	--NONE--

Commands

aaa profile "US-Guest-AAA"

initial-role guest-login

Hide Commands

Create Open SSID

Monitoring

Configuration

Diagnostics

Maintenance

Plan

Events

Reports

Licenses will expire in 30 days

Save Configuration

Log

Network

Controller

VLANs

Ports

IP

Security

Authentication

Access Control

Wireless

AP Configuration

AP Installation

Management

General

Administration

Certificates

SNMP

Logging

Clock

Advanced Services

Redundancy

IP Mobility

Stateful Firewall

External Services

Wired Access

Wireless

All Profiles

Advanced Services > All Profile Management

Profiles

+ AP

+ RF Management

- Wireless LAN

- SSID Profile

+ default

+ Employee-SSID

- Guest-SSID

+ Virtual AP profile

+ AAA Profile

+ XML API Server

+ RFC 3576 Server

+ MAC Authentication Profile

Profile Details

SSID Profile > Guest-SSID

Save As

Reset

Basic

Advanced

Network

Network Name (SSID)

Guest

802.11 Security

Network Authentication

☒ None

☐ 802.1x/WEP

☐ WPA

☐ WPA-PSK

☐ WPA2

☐ WPA2-PSK

☐ Mixed

Encryption

☒ Open

☐ WEP

Keys

Assign SSID and AAA Profiles to VAP

Monitoring

Configuration

Diagnostics

Maintenance

Plan

Events

Reports

Licenses will expire in 30 days

Save Configuration

Log

Network

Controller

VLANs

Ports

IP

Security

Authentication

Access Control

Wireless

AP Configuration

AP Installation

Management

General

Administration

Certificates

SNMP

Logging

Clock

Advanced Services

Redundancy

IP Mobility

Stateful Firewall

External Services

Wired Access

Configuration > AP Group > Edit "US Building 2"

Profiles

Wireless LAN

Virtual AP

US-Corp-Employee-VAP

US-Guest-VAP

SSID Profile

Guest-SSID

AAA Profile

US-Guest-AAA

RF Management

AP

QOS

IDS

Profile Details

AAA Profile > US-Guest-AAA

Save As

Reset

Initial role	guest-login	MAC Authentication Default Role	guest
802.1X Authentication Default Role	guest	User derivation rules	--NONE--
Wired to Wireless Roaming	<input checked="" type="checkbox"/>	SIP authentication role	--NONE--

MAC Authentication Profile

MAC Authentication Server Group

802.1X Authentication Profile

802.1X Authentication Server Group

RADIUS Accounting Server Group

XML API server

RFC 3576 server

default

Apply

Customize Captive Portal Page

Monitoring	Configuration	Diagnostics	Maintenance	Plan	Events	Reports	Licenses will expire in 29 days	Logout
------------	---------------	-------------	-------------	------	--------	---------	---------------------------------	--------

Controller

- Image Management
- Reboot Controller
- Clear Config
- Synchronize Database
- Boot Parameters

File

- Copy Files
- Copy Logs
- Copy Crash Files
- Backup Flash
- Restore Flash
- Delete Files

WLAN

- Reboot AP
- WMS Database

Captive Portal


- Customize Login Page**
- Upload Custom Login Pages

Captive Portal > Customize Login Page


Profile:

Customize the look of your Captive Portal

Page Design:
(Click your choice.)



Logo



YOUR CUSTOM
BACKGROUND

JPEG FORMAT ONLY

Page text (in HTML format):
(Size limited to 16K)

Additional options

Upload your own logo:
(Logo dimensions must be 176px
wide by 46px high or smaller.)

Browse...

Edit your Acceptable Use Policy

Policy Text (in HTML format):
(Used only when Guest Access is
enabled. Size limited to 32K)

Submit

Reset

[View CaptivePortal](#)

- Aruba supports 2 VPN types
 - PPTP (widely supported, Windows, Mac, Unix, PDA)
 - L2TP over IPSec (Windows 2000 and XP, Mac OSX, Unix)
- Protocol details are outside the scope of this course but both utilize strong encryption
- May authenticate against internal or external server
- After successful authentication, Role assigned



VPN Configuration Steps

Step 1: Configure the external auth-server or internal-db

Step 2: Create a server group and assign the configured auth-server to it.

Step 3: Create a VPN Auth profile and select the Default Role and Server Group

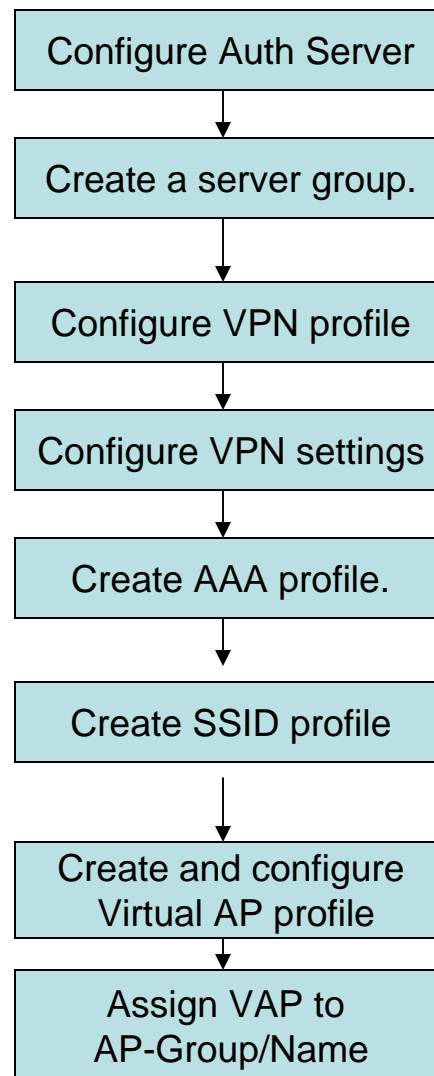
Step 4: Configure VPN-specific parameters (PPTP and IPSec)

Step 5: Create a AAA profile and select an Initial Role that contains the vpnlogin FW policy.

Step 6: Create an SSID profile and configure the required opmode to use with VPN (typically open), SSID name, and other parameters.

Step 7: Create a Virtual AP profile and assign the AAA and SSID profiles previously created to it.

Step 8: Assign the Virtual AP to an AP Group/AP Name.



VPN Configuration

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Licenses will expire in 23 days Save Configuration Log

Network
Controller
VLANs
Ports
IP

Security
Authentication
Access Control

Wireless
AP Configuration
AP Installation

Management
General
Administration
Certificates
SNMP
Logging
Clock

Advanced Services
Redundancy
IP Mobility
Stateful Firewall
VPN Services
Wired Access

Security > Authentication > L3 Authentication

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

☒ Captive Portal Authentication Profile

☐ VPN Authentication Profile

Server Group default

Default Role Employee Max Authentication failures 0

Specify Server group and Default Role

Apply

L2TP Configuration

Advanced Services > VPN Services > IPSEC

IPSEC

PPTP

Dialers

Emulate VPN Servers

Site-To-Site

Advanced

L2TP and XAUTH Parameters

Enable L2TP	<input checked="" type="checkbox"/>
Authentication Protocols	<input checked="" type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MSCHAP <input type="checkbox"/> MSCHAPv2
Primary DNS Server	<input type="text" value="10.54.36.82"/>
Secondary DNS Server	<input type="text" value="10.54.40.10"/>
Primary WINS Server	<input type="text" value="0.0.0.0"/>
Secondary WINS Server	<input type="text" value="0.0.0.0"/>

Address Pools

Pool Name	Start Address	End Address	Actions
RemoteVPN	192.168.44.100	192.168.44.150	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="button" value="Add"/>			

Source NAT

Enable Source NAT	<input type="checkbox"/>
NAT Pool	<input type="button" value="v"/>

Aggressive Mode

IKE Aggressive Group Name	<input type="text" value="changeme"/> (Only needed for XAUTH)
---------------------------	---

IKE Shared Secrets

Subnet	Subnet Mask Length	Key	Actions
<input type="button" value="Add"/>			

IKE Policies

Priority	Encryption	Hash	Authentication	Group	Lifetime(secs)	Action
Default	3DES	SHA	PRE-SHARE	GROUP 2	[300 - 86400]	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="button" value="Add"/>						

PPTP Configuration

Advanced Services > VPN Services > PPTP

[IPSEC](#)[PPTP](#)[Dialers](#)[Emulate VPN Servers](#)[Site-To-Site](#)[Advanced](#)

PPTP Parameters

Enable PPTP	<input checked="" type="checkbox"/>
PPTP Echo Timeout(secs)	<input type="text" value="60"/>
Authentication Protocols	<input checked="" type="checkbox"/> MSCHAPv2
Primary DNS Server	<input type="text" value="10.54.36.82"/>
Secondary DNS Server	<input type="text" value="10.54.41.10"/>
Primary WINS Server	<input type="text" value="0.0.0.0"/>
Secondary WINS Server	<input type="text" value="0.0.0.0"/>

Address Pools

Pool Name	Start Address	End Address	Actions	
RemoteVPN	192.168.44.100	192.168.44.150	Edit	Delete

[Add](#)[Apply](#)



VPN Dialer

- Captive Portal may be used for authentication
- For Windows users, a 'dialer' application may be downloaded directly from the switch following successful Captive Portal authentication
- Can be manually installed
- Pre-configured to work with Aruba
 - Configuration depends on role
 - Can set different groups to PPTP and IPSec
- Has wired detection feature which can disable wireless access when device is plugged in

- Standard protocol for authenticating user *prior* to granting access to L2 media
- Utilizes EAP (Extensible Authentication Protocol)
 - Evolved from PPP, used for wired network authentication - unencrypted
 - Several types of “Wireless” EAP
 - Cisco LEAP
 - EAP-TLS
 - PEAP
 - EAP-TTLS
 - These sub-types intended for use on untrusted networks such as wireless

Supplicant: client station

Authenticator: Aruba controller

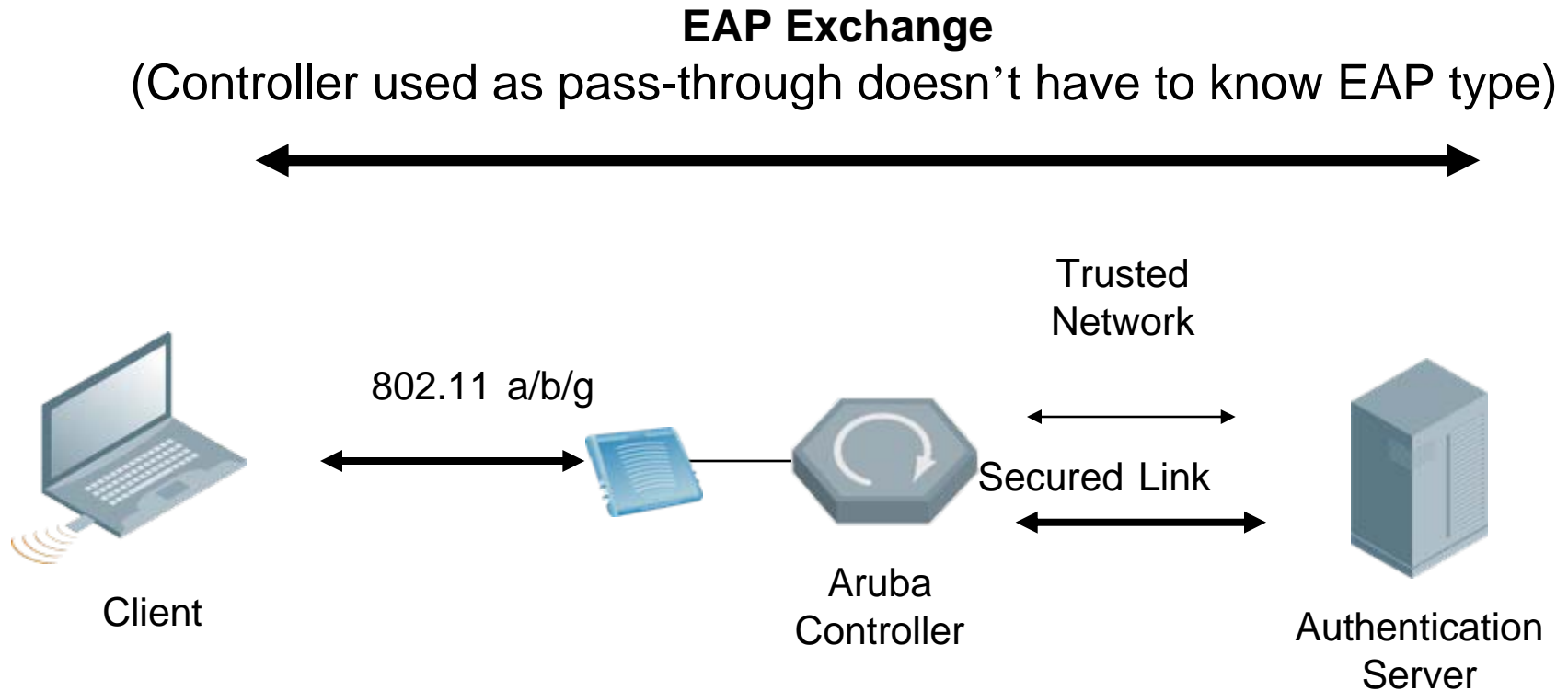
Authentication Server: RADIUS Server



EAP Overview

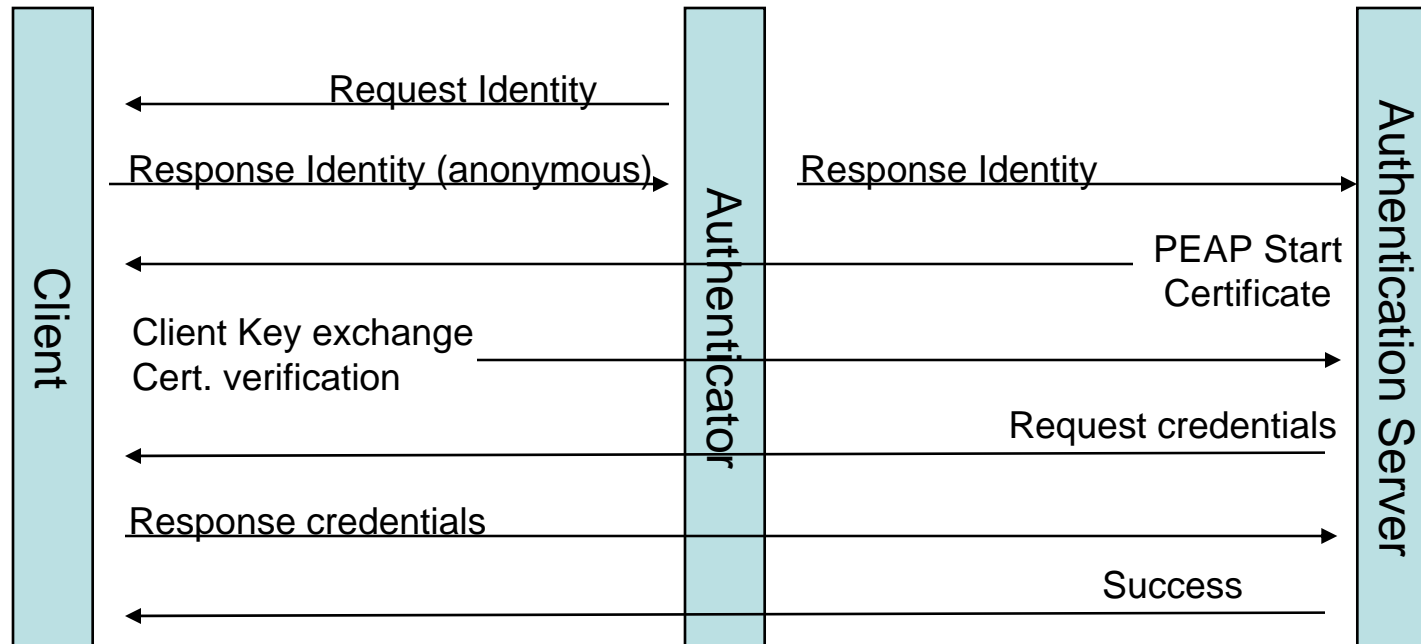
1. Supplicant communicates with authentication server **through** the authenticator
2. Authenticator reformats 802.1x to RADIUS and forwards to Authentication Server
3. EAP exchange happens between supplicant and authentication server
4. On success, server delivers EAP Success via RADIUS message
5. Details often hidden from authenticator
6. The Aruba controller is EAP agnostic

EAP Exchange



802.1x Process

802.1x Access Control – Sequence of events





EAP Flavors

LEAP

- Cisco proprietary
- Dynamic WEP
- Has been broken. Not recommended for current deployment

EAP-TLS (EAP with Transport Layer Security)

- RFC 2716 - based on SSL
- Uses both client and server certificates
- Provides for mutual authentication
- Supported by Windows 2000, XP, 3rd party clients

EAP-PEAP

- Based on TLS
- Hides EAP exchange
- Requires both server and client authentication
- Developed by Microsoft, Cisco and RSA Security

EAP-FAST

- Cisco proprietary
- Uses a PSK in phase 0 to obtain a PAC file, PAC is used as credentials on network
- Subject to man in the middle attacks; poor Windows AD integration

EAP-TTLS

- Similar to PEAP, but allows for any EAP authentication protocol
- Requires 3rd party client
- Developed by Funk Software



Configuring an SSID to use dot1x

Step 1: Configure the external auth-server or internal-db

Step 2: Create a server group and assign the configured auth-server to it.

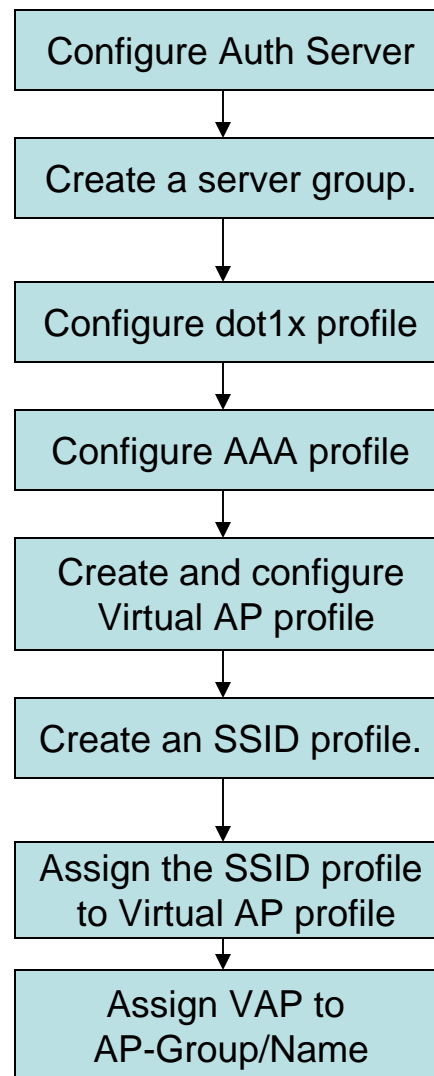
Step 3: Create a dot1x profile and configure the required dot1x parameters (EAP-Offload, Key rotation, re-auth, etc.)

Step 4: Create a AAA profile and assign the dot1x profile and dot1x server-groups created in Steps 2 and 3.

Step 5: Create an SSID profile and configure the required opmode to use with dot1x, SSID name and other parameters.

Step 6: Create a Virtual AP profile and assign the AAA and SSID profiles previously created to it.

Step 7: Assign the Virtual AP to an AP Group/AP Name.



802.1x Configuration

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Licenses will expire in 30 days Save Configuration Log

Network
Controller
VLANs
Ports
IP

Security
Authentication
Access Control

Wireless
AP Configuration
AP Installation

Management
General
Administration
Certificates
SNMP
Logging
Clock

Advanced Services
Redundancy
IP Mobility
Stateful Firewall
External Services
Wired Access
Wireless

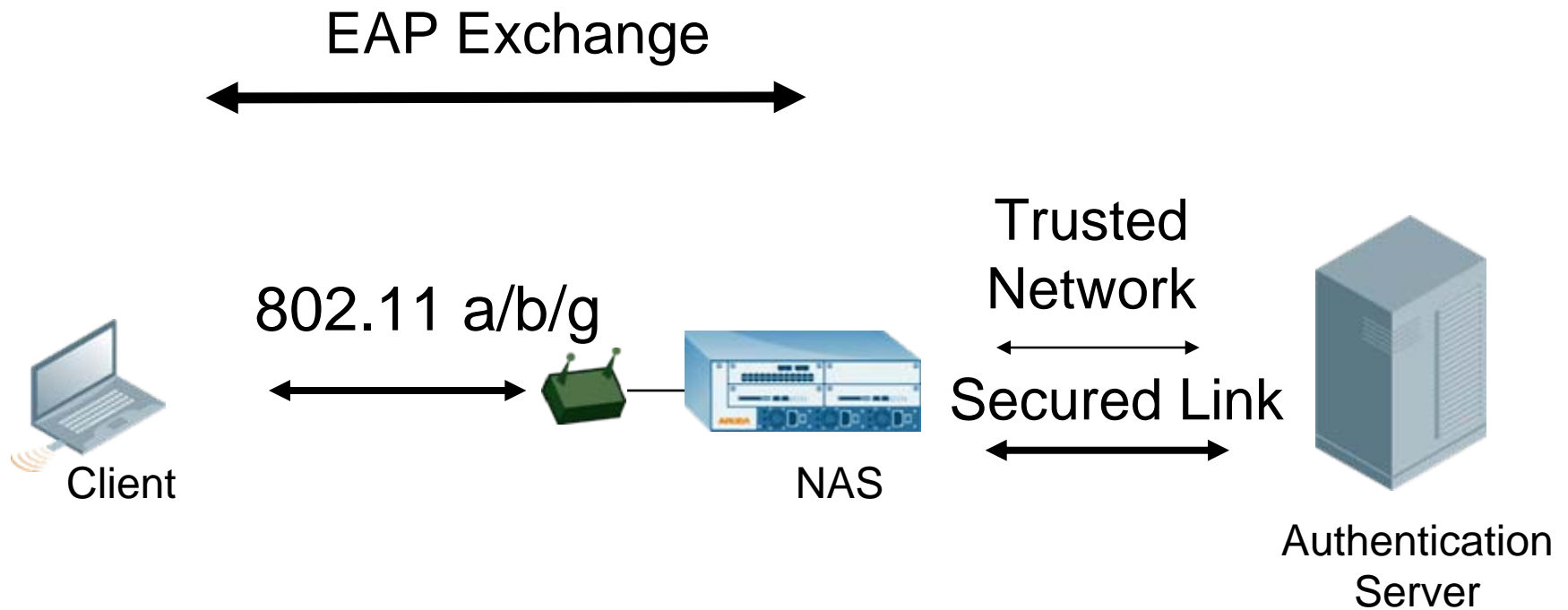
All Profiles

Advanced Services > All Profile Management

Profiles	Profile Details																
<ul style="list-style-type: none">Virtual AP profileAAA ProfileXML API ServerRFC 3576 ServerMAC Authentication ProfileCaptive Portal Authentication Profile802.1X Authentication Profile<ul style="list-style-type: none">defaultdefault-pskRADIUS ServerLDAP Server	<div>802.1X Authentication Profile > default Save As Reset</div> <div>Basic Advanced</div> <table border="1"><tbody><tr><td>Max authentication failures</td><td>0</td></tr><tr><td>Enforce Machine Authentication</td><td><input type="checkbox"/></td></tr><tr><td>Machine Authentication: Default Machine Role</td><td>guest</td></tr><tr><td>Machine Authentication: Default User Role</td><td>guest</td></tr><tr><td>Reauthentication</td><td><input type="checkbox"/></td></tr><tr><td>Termination</td><td><input type="checkbox"/></td></tr><tr><td>Termination EAP-Type</td><td><input type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-peap</td></tr><tr><td>Termination EAP-Type</td><td><input type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-mschapv2</td></tr></tbody></table> <div>Apply View Commands</div>	Max authentication failures	0	Enforce Machine Authentication	<input type="checkbox"/>	Machine Authentication: Default Machine Role	guest	Machine Authentication: Default User Role	guest	Reauthentication	<input type="checkbox"/>	Termination	<input type="checkbox"/>	Termination EAP-Type	<input type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-peap	Termination EAP-Type	<input type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-mschapv2
Max authentication failures	0																
Enforce Machine Authentication	<input type="checkbox"/>																
Machine Authentication: Default Machine Role	guest																
Machine Authentication: Default User Role	guest																
Reauthentication	<input type="checkbox"/>																
Termination	<input type="checkbox"/>																
Termination EAP-Type	<input type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-peap																
Termination EAP-Type	<input type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-mschapv2																

Select Profile and provision 802.1x parameters. Remember to set server group too.

EAP-Offload



EAP Offload (continued)

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Licenses will expire in 30 days Save Configuration Logout

Advanced Services > All Profile Management

Profiles	Profile Details																
<ul style="list-style-type: none">+ AP+ RF Management- Wireless LAN<ul style="list-style-type: none">+ SSID Profile+ Virtual AP profile+ AAA Profile+ XML API Server+ RFC 3576 Server+ MAC Authentication Profile+ Captive Portal Authentication Profile- 802.1X Authentication Profile<ul style="list-style-type: none">default	<div>802.1X Authentication Profile > default Save As Reset</div> <div>Basic Advanced</div> <table border="1"><tbody><tr><td>Max authentication failures</td><td>0</td></tr><tr><td>Enforce Machine Authentication</td><td><input type="checkbox"/></td></tr><tr><td>Machine Authentication: Default Machine Role</td><td>guest</td></tr><tr><td>Machine Authentication: Default User Role</td><td>guest</td></tr><tr><td>Reauthentication</td><td><input type="checkbox"/></td></tr><tr><td>Termination</td><td><input checked="" type="checkbox"/></td></tr><tr><td>Termination EAP-Type</td><td><input type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-peap</td></tr><tr><td>Termination Inner EAP-Type</td><td><input type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-mschapv2</td></tr></tbody></table>	Max authentication failures	0	Enforce Machine Authentication	<input type="checkbox"/>	Machine Authentication: Default Machine Role	guest	Machine Authentication: Default User Role	guest	Reauthentication	<input type="checkbox"/>	Termination	<input checked="" type="checkbox"/>	Termination EAP-Type	<input type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-peap	Termination Inner EAP-Type	<input type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-mschapv2
Max authentication failures	0																
Enforce Machine Authentication	<input type="checkbox"/>																
Machine Authentication: Default Machine Role	guest																
Machine Authentication: Default User Role	guest																
Reauthentication	<input type="checkbox"/>																
Termination	<input checked="" type="checkbox"/>																
Termination EAP-Type	<input type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-peap																
Termination Inner EAP-Type	<input type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-mschapv2																

Apply

Commands

[Hide Commands](#)

```
aaa authentication dot1x "default"  
termination enable
```

Encryption



ARUBATM
The **Mobile Edge** Company

Configuring 802.1x/802.11i

Monitoring

Configuration

Diagnostics

Maintenance

Plan

Events

Reports

Licenses will expire in 30 days

Save Configuration

Log

Network

Controller

VLANs

Ports

IP

Security

Authentication

Access Control

Wireless

AP Configuration

AP Installation

Management

General

Administration

Certificates

SNMP

Logging

Clock

Advanced Services

Redundancy

IP Mobility

Stateful Firewall

External Services

Wired Access

Wireless

All Profiles

Advanced Services > All Profile Management

Profiles

Profile Details

+

 AP

+

 RF Management

-

 Wireless LAN

-

 SSID Profile

+

 default

-

 Employee-SSID

+

 Guest-SSID

+

 Virtual AP profile

+

 AAA Profile

+

 XML API Server

+

 RFC 3576 Server

+

 MAC Authentication Profile

SSID Profile > Employee-SSID

Save As

Reset

Basic

Advanced

Network

Network Name (SSID)

Employee

802.11 Security

Network Authentication

None

802.1x/WEP

WPA

WPA-PSK

WPA2

WPA2-PSK

Mixed

Encryption

AES

Keys

Commands

Apply

View Commands

ARUBA™

The Mobile Edge Company

Confidential

©2005 All rights reserved

Guest Provisioning



ARUBATM
The **Mobile Edge** Company



Aruba Guest Provisioning

- Aruba offers a mechanism for managing guest accounts
- A guest provisioning management account presents a security guard or receptionist with a minimal user interface in order to manage entries in the Internal Database
- Temporary guest accounts can then be created as guests arrive and set to automatically expire at a predetermined time

Create Guest Provisioning Account

- Create the admin account to be used by the guard or receptionist to log into the Aruba Controller

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Licenses will expire in 29 days Save Configuration Logout

Network
Controller
VLANs
Ports
IP

Security
Authentication
Access Control

Wireless
AP Configuration
AP Installation

Management
General
Administration
Certificates
SNMP
Logging
Clock

Advanced Services
Redundancy
IP Mobility
Stateful Firewall
VPN Services
Wired Access
Wireless
All Profiles

Management > Administration > Add User [« Back](#)

Add User

☒ Conventional User Accounts

User Name:

Password:

Confirm Password:

Role:

☐ Certificate Management

☐ WebUI Certificate

Username:

Role:

Client Certificate Serial No.:

Trusted CA Certificate Name:

☐ SSH Public Key ☐ Copy The WebUI Certificate Management Information (username and role)

Username:

Role:

Client Certificate name:

[Apply](#)

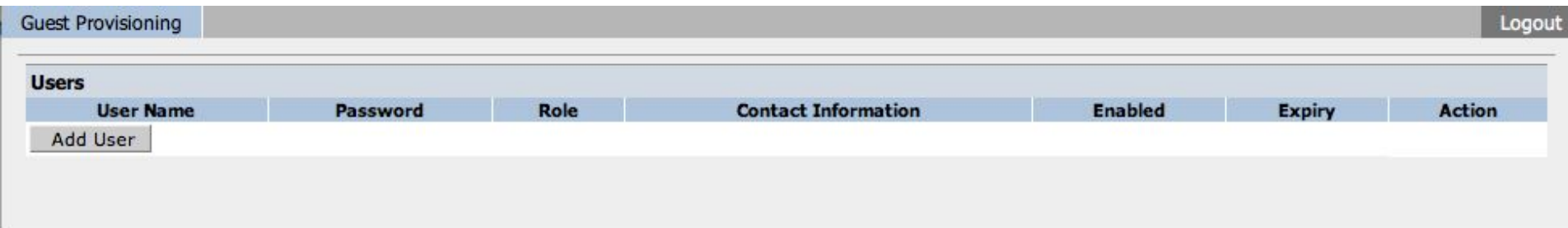
Commands

[Hide Commands](#)

```
mgmt-user "receptionist" "guest-provisioning" *****
```

Guest Provisioning Interface

1) Log in to the controller using the Guest Provisioning Account

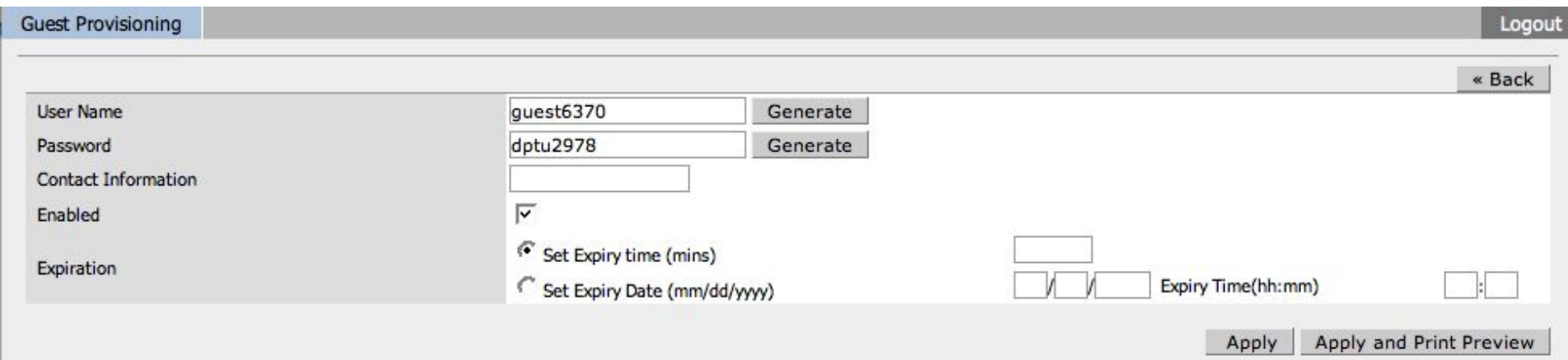


The screenshot shows the 'Guest Provisioning' interface. At the top, there is a 'Guest Provisioning' tab and a 'Logout' link. Below this is a table titled 'Users' with columns: 'User Name', 'Password', 'Role', 'Contact Information', 'Enabled', 'Expiry', and 'Action'. Below the table is an 'Add User' button.

User Name	Password	Role	Contact Information	Enabled	Expiry	Action
-----------	----------	------	---------------------	---------	--------	--------

Add User

2) Click Add User, enter user info, and click “Apply and Print Preview



The screenshot shows the 'Guest Provisioning' interface with the 'Add User' form. The form has fields for 'User Name', 'Password', 'Contact Information', 'Enabled', and 'Expiration'. The 'User Name' field contains 'guest6370' and the 'Password' field contains 'dptu2978'. There are 'Generate' buttons next to these fields. The 'Contact Information' field is empty. The 'Enabled' field has a checked checkbox. The 'Expiration' field has two radio buttons: 'Set Expiry time (mins)' and 'Set Expiry Date (mm/dd/yyyy)'. The 'Set Expiry time (mins)' field has a value of '15'. The 'Set Expiry Date (mm/dd/yyyy)' field has a value of '1/1/2010'. There is an 'Expiry Time(hh:mm)' field with a value of '1:00'. At the bottom right, there are 'Apply' and 'Apply and Print Preview' buttons.

User Name: guest6370 Generate

Password: dptu2978 Generate


Contact Information:


Enabled: ☒

Expiration: ☒ Set Expiry time (mins) 15 ☐ Set Expiry Date (mm/dd/yyyy) 1/1/2010 Expiry Time(hh:mm) 1:00

Apply Apply and Print Preview

Guest Provisioning cont.


The **Mobile Edge** Company



Username	guest1382
Password	ynyx2043
Expiration date/time	Unknown

Terms and Conditions

Welcome to the Aruba Networks Web site which includes the support site and partner sites (the "Site"). By using the Site, you agree to follow and be bound by the following terms and conditions concerning your use of the Site ("Terms of Use") and our Privacy Policy. We may revise the Terms of Use and Privacy Policy at any time without notice to you.

Print

Customizing Guest Provisioning

Monitoring

Configuration

Diagnostics

Maintenance

Plan

Events

Reports

Licenses will expire in 29 days

Save Configuration

Logout

Network

Controller

VLANs

Ports

IP

Security

Authentication

Access Control

Wireless

AP Configuration

AP Installation

Management

General

Administration

Certificates

SNMP

Logging

Clock

Advanced Services

Redundancy

IP Mobility

Stateful Firewall

VPN Services

Wired Access

Security > Access Control > Customize Guest Access Page

User Roles

System Roles

Policies

Time Ranges

Guest Access

Customize the look of your Guest Access Pass

Upload your company logo

Browse...

Username

[username]

Password

[password]

Expiration date/time

[date/time]

Policy text (in HTML format)

Submit

Reset

Preview Pass



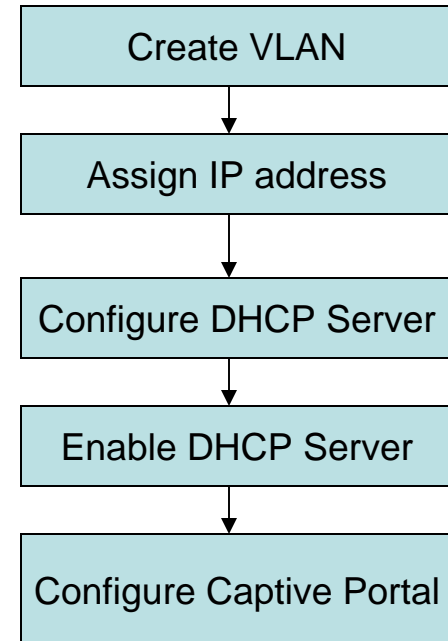
Guest Access Configuration Steps

Step 1: Create user VLAN and assign IP address

Step 2: Configure DHCP server

Step 3: Enable DHCP server

Step 4: Configure Captive Portal





Captive Portal Configuration Steps

Step 1: Configure the auth-server (external or internal-db)

Step 2: Create a server group and assign the configured auth-server to it.

Step 3: Create a Captive Portal profile and configure the required parameters (default role, server group, etc.)

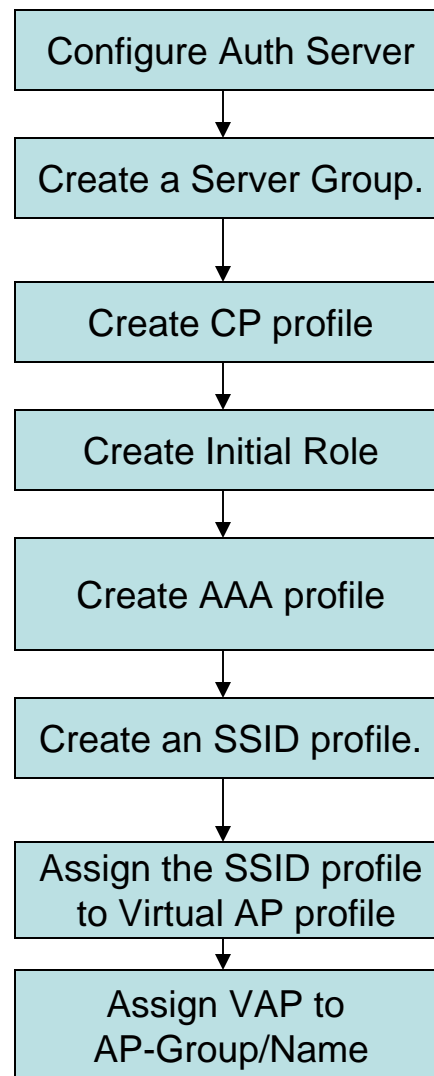
Step 4: Create an Initial Role and assign the Captive Portal profile

Step 5: Create a AAA profile and assign the Initial Role.

Step 6: Create an SSID profile and configure the required encryption (open), SSID name, and other parameters.

Step 7: Create a Virtual AP profile and assign the AAA and SSID profiles previously created to it.

Step 8: Assign the Virtual AP to an AP Group/AP Name.



Master-Local and Mobility

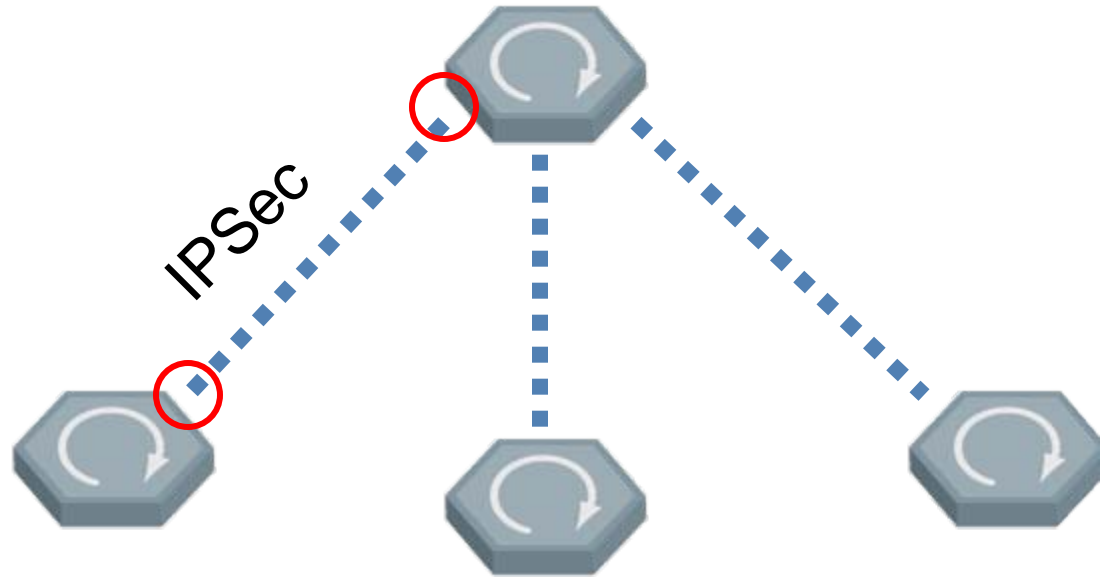


ARUBATM

The **Mobile Edge** Company

Master-Local IPSec Tunnel

- An IPSec Tunnels are automatically created between the Master and each Local for inter-controller communication
- Built from the Local to the Master using the switchip
- Can use default PSK, or create unique PSK pairs




On the master controller:

```
localip ipaddr ipsec key
```

On the local controller:

```
masterip ipaddr ipsec key
```

Intercontroller IPSec Setup



Monitoring Configuration Diagnostics Maintenance Plan Events Reports

Network

- Controller
- VLANs
- Ports
- IP

Security

- Authentication
- Access Control

Wireless

- AP Configuration
- AP Installation

Management

- General
- Administration
- Certificates
- SNMP

Network > Controller > System Settings

System Settings Licenses

Controller Role	Master
Master IP Address	192.168.2.80
IPSec Key (IKE PSK)	
Retype IPSec Key (IKE PSK)	

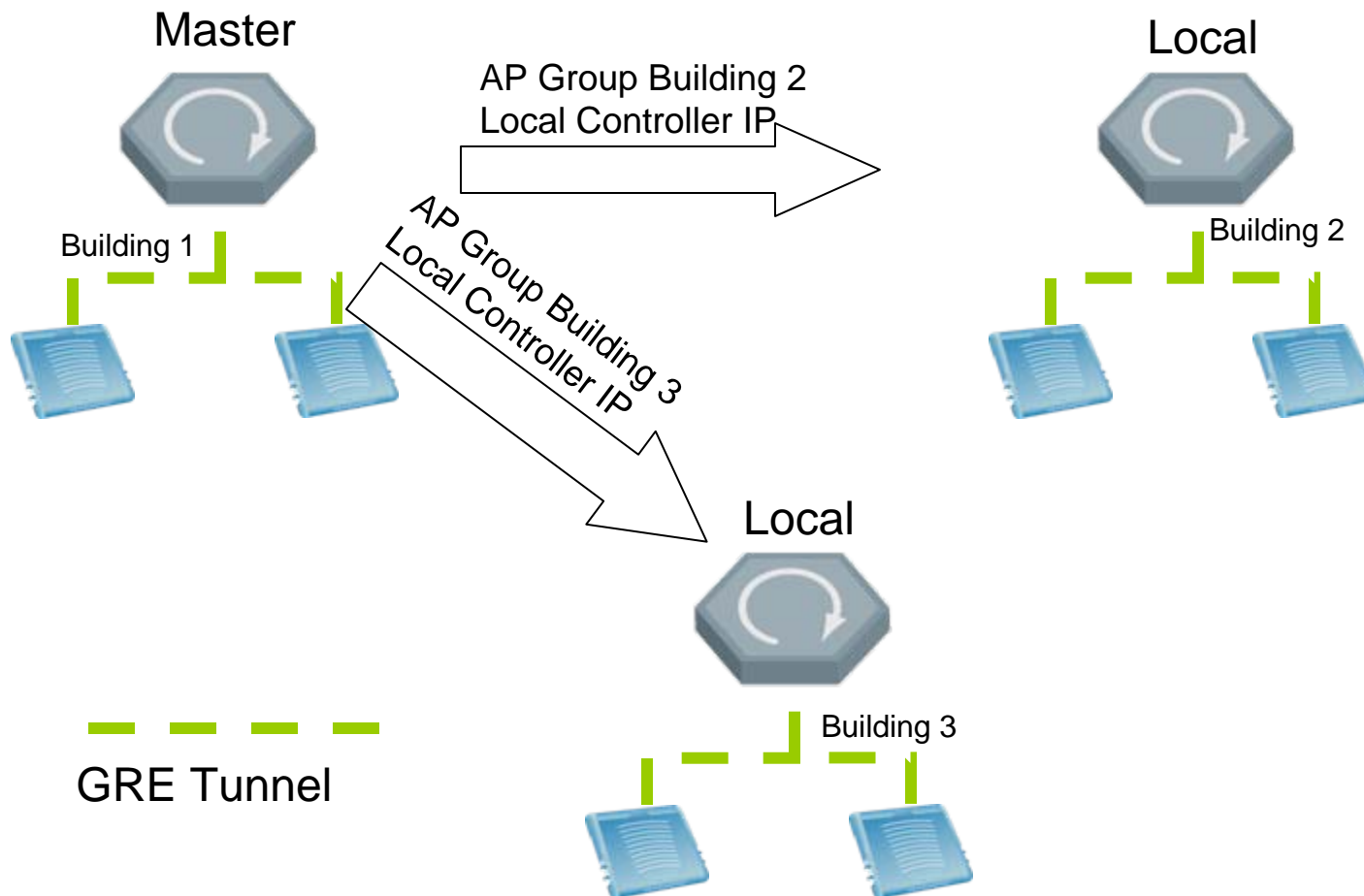
Local Controller IPSec Keys

Local Controller IP Address	Key		
0.0.0.0	*****	Edit	Delete
192.168.2.80	*****	Edit	Delete

New

Use default key, or
create unique pairs

Multi-Controller



Configure APs for Multi-Controller

- Point lms-ip to local controllers

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Save Configuration Logout

Network
Controller
VLANs
Ports
IP

Security
Authentication
Access Control

Wireless
AP Configuration
AP Installation

Management
General
Administration
Certificates
SNMP
Logging
Clock

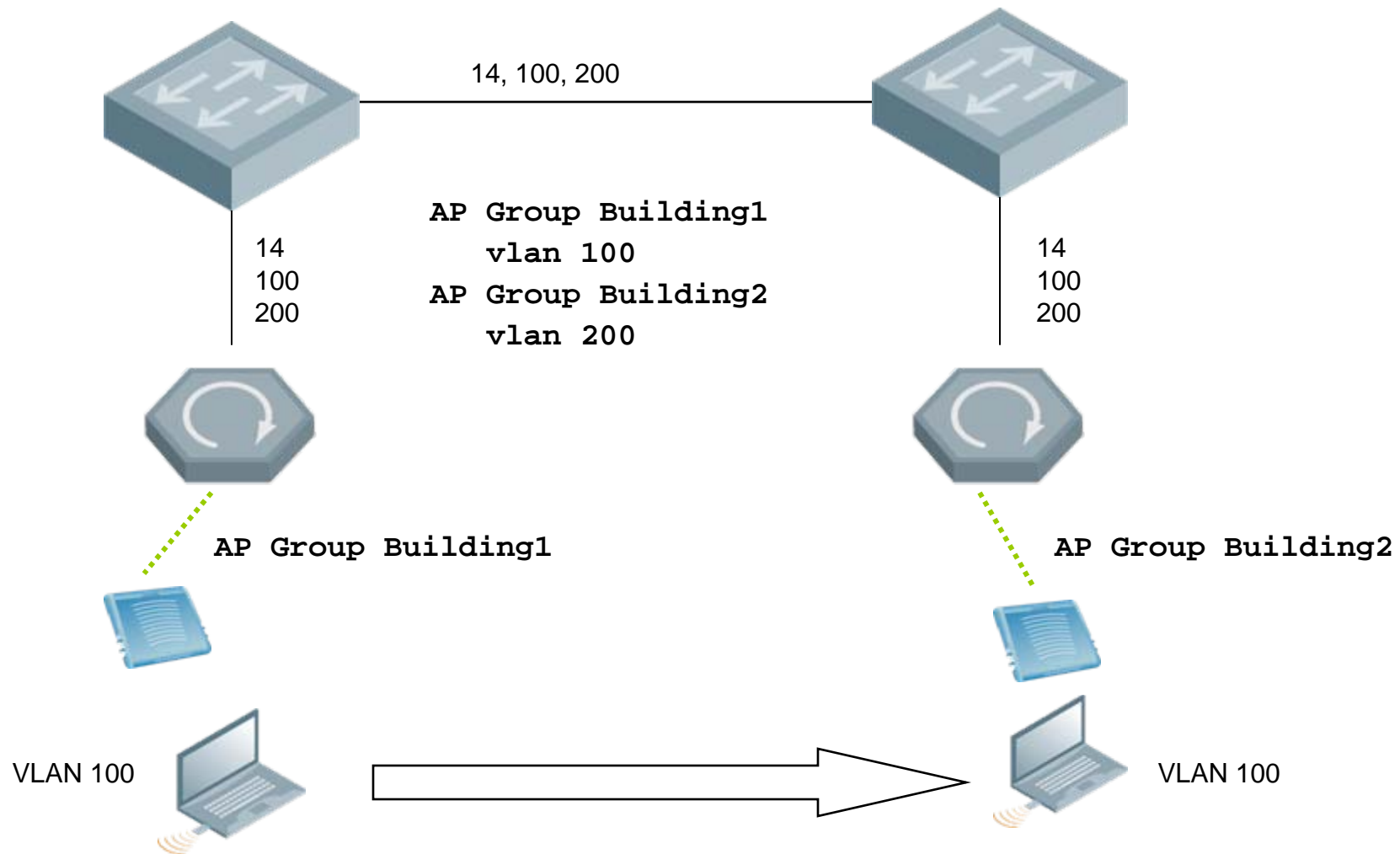
Advanced Services
Redundancy
IP Mobility
Wired Access
Wireless
All Profiles

Configuration > AP Group > Edit "Building2"

Profiles		Profile Details																																	
<div>Wireless LAN</div> <div>RF Management</div> <div>AP</div> <div>Wired AP profile default</div> <div>Ethernet interface 0 link profile default</div> <div>Ethernet interface 1 link profile default</div> <div>AP system profile Building2</div> <div>Regulatory Domain profile default</div> <div>SNMP profile default</div> <div>QOS</div> <div>IDS</div>		<div>AP system profile > Building2</div> <div>Save As Reset</div> <table><tr><td>LMS IP</td><td>10.1.19.101</td><td>Backup LMS IP</td><td></td></tr><tr><td>Master switch IP address</td><td></td><td>RF Band</td><td>g</td></tr><tr><td>Double Encrypt</td><td><input type="checkbox"/></td><td>Native VLAN ID</td><td>1</td></tr><tr><td>SAP MTU</td><td></td><td>bytes</td><td>Bootstrap threshold 8</td></tr><tr><td>Request Retry Interval</td><td>10</td><td>sec</td><td>Maximum Request Retries 10</td></tr><tr><td>Keepalive Interval</td><td>60</td><td>sec</td><td>Dump Server</td></tr><tr><td>Telnet</td><td><input type="checkbox"/></td><td>SNMP sysContact</td><td></td></tr><tr><td>AeroScout RTLS</td><td>addr</td><td></td><td></td></tr></table>		LMS IP	10.1.19.101	Backup LMS IP		Master switch IP address		RF Band	g	Double Encrypt	<input type="checkbox"/>	Native VLAN ID	1	SAP MTU		bytes	Bootstrap threshold 8	Request Retry Interval	10	sec	Maximum Request Retries 10	Keepalive Interval	60	sec	Dump Server	Telnet	<input type="checkbox"/>	SNMP sysContact		AeroScout RTLS	addr		
LMS IP	10.1.19.101	Backup LMS IP																																	
Master switch IP address		RF Band	g																																
Double Encrypt	<input type="checkbox"/>	Native VLAN ID	1																																
SAP MTU		bytes	Bootstrap threshold 8																																
Request Retry Interval	10	sec	Maximum Request Retries 10																																
Keepalive Interval	60	sec	Dump Server																																
Telnet	<input type="checkbox"/>	SNMP sysContact																																	
AeroScout RTLS	addr																																		

Apply

Layer 2 Mobility



Enabling Inter-Controller L2 Mobility

Monitoring

Configuration

Diagnostics

Maintenance

Plan

Events

Reports

Licenses will expire in 30 days

Save Configuration

Log

Network

Controller

VLANs

Ports

IP

Security

Authentication

Access Control

Wireless

AP Configuration

AP Installation

Management

General

Administration

Certificates

SNMP

Logging

Clock

Advanced Services

Redundancy

IP Mobility

Stateful Firewall

External Services

Wired Access

Wireless

All Profiles

Advanced Services > All Profile Management

Profiles

+ AP

+ RF Management

- Wireless LAN

+ SSID Profile

- Virtual AP profile

+ default

+ EMEA-Corp-Employee-VAP

- US-Corp-Employee-VAP

+ SSID Profile Employee-SSID

+ AAA Profile US-Employee-AAA

+ US-Guest-VAP

+ AAA Profile

+ XML API Server

Profile Details

Virtual AP profile > US-Corp-Employee-VAP

Virtual AP enable

☒

Allowed band

all

VLAN

109

<--

Forward mode

tunnel

Deny time range

--NONE--

Mobile IP

☒

DoS Prevention

☐

Station Blacklisting

☒

Blacklist Time

3600

sec

Authentication Failure Blacklist Time

3600

Fast Roaming

☐

Strict Compliance

☐

VLAN Mobility

☒

Save As

F

Apply

Commands

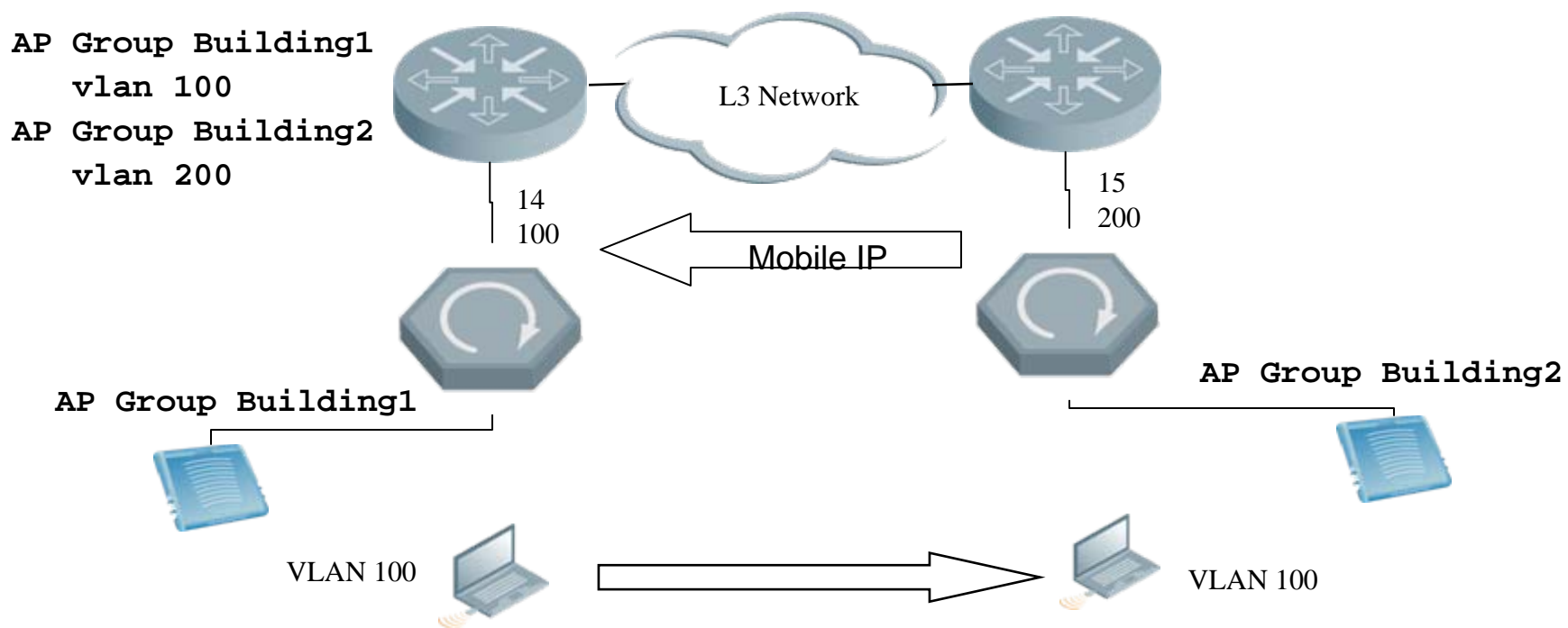
Hide Commands

wlan virtual-ap "US-Corp-Employee-VAP"

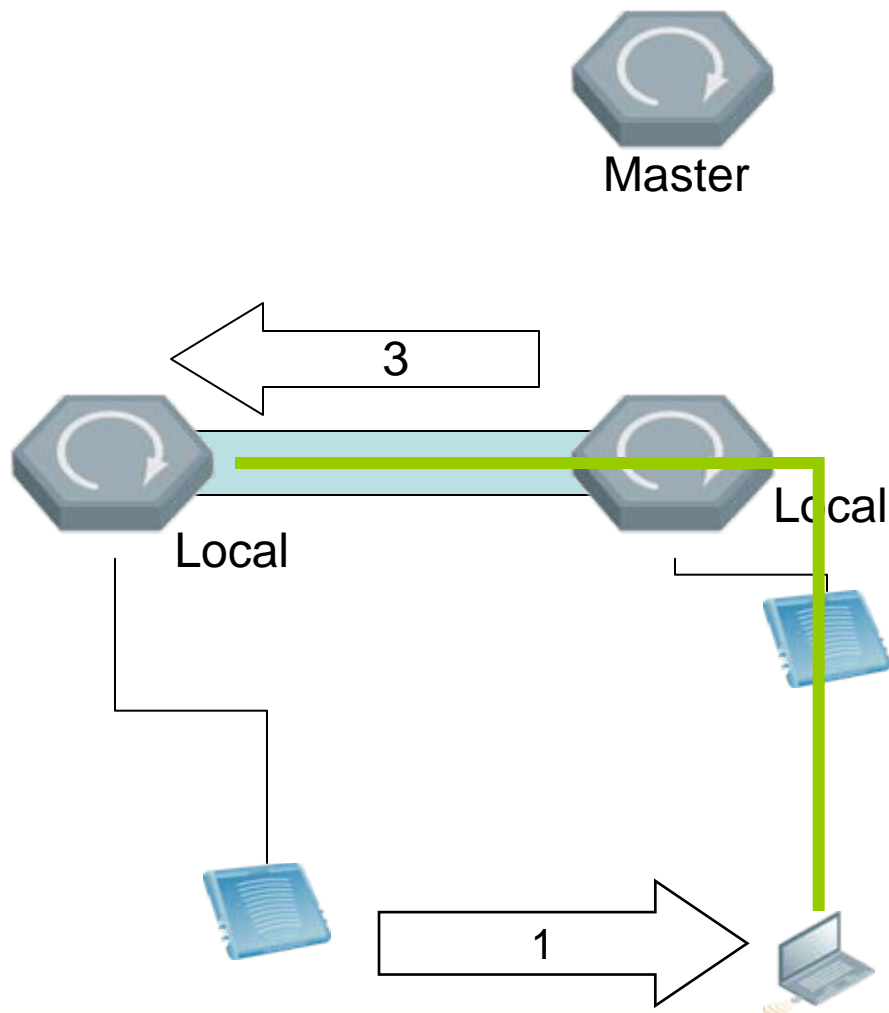
vlan-mobility

Layer 3 Mobility

- L3 mobility should be enabled when controllers are separated by an L3 network
- Controllers build mobile-IP tunnels to transmit client traffic to original controller (home agent)



Inter-Controller Mobility



1. Client roams to different controller (foreign agent)
2. FA recognizes client
3. FA builds tunnel to HA
4. Client's traffic tunneled through HA to destination



Mobility Domains

- Domains define a boundary for roaming clients
- Generally a controller belongs to one domain, although it can belong to more
- Domains defined as controllers and supported subnets
- Mobility Domains and Home Agent Tables (HATs) are Provisioned on Master Controller and pushed to Locals



Mobility Domains

Building 1



Master



Local

Building 2

Local



Local



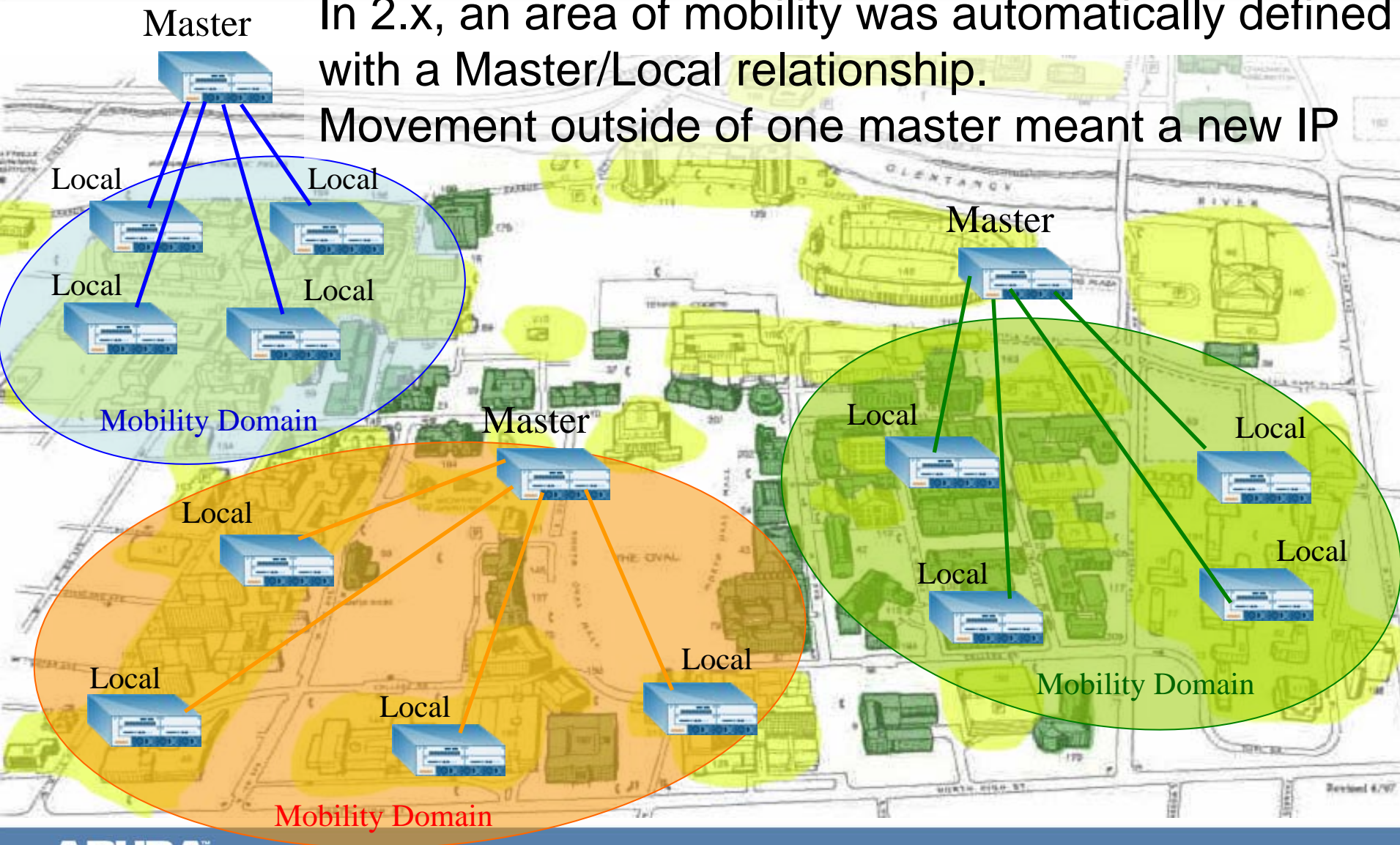
Local





Deploying Mobility Over Large Areas AOS 2.x

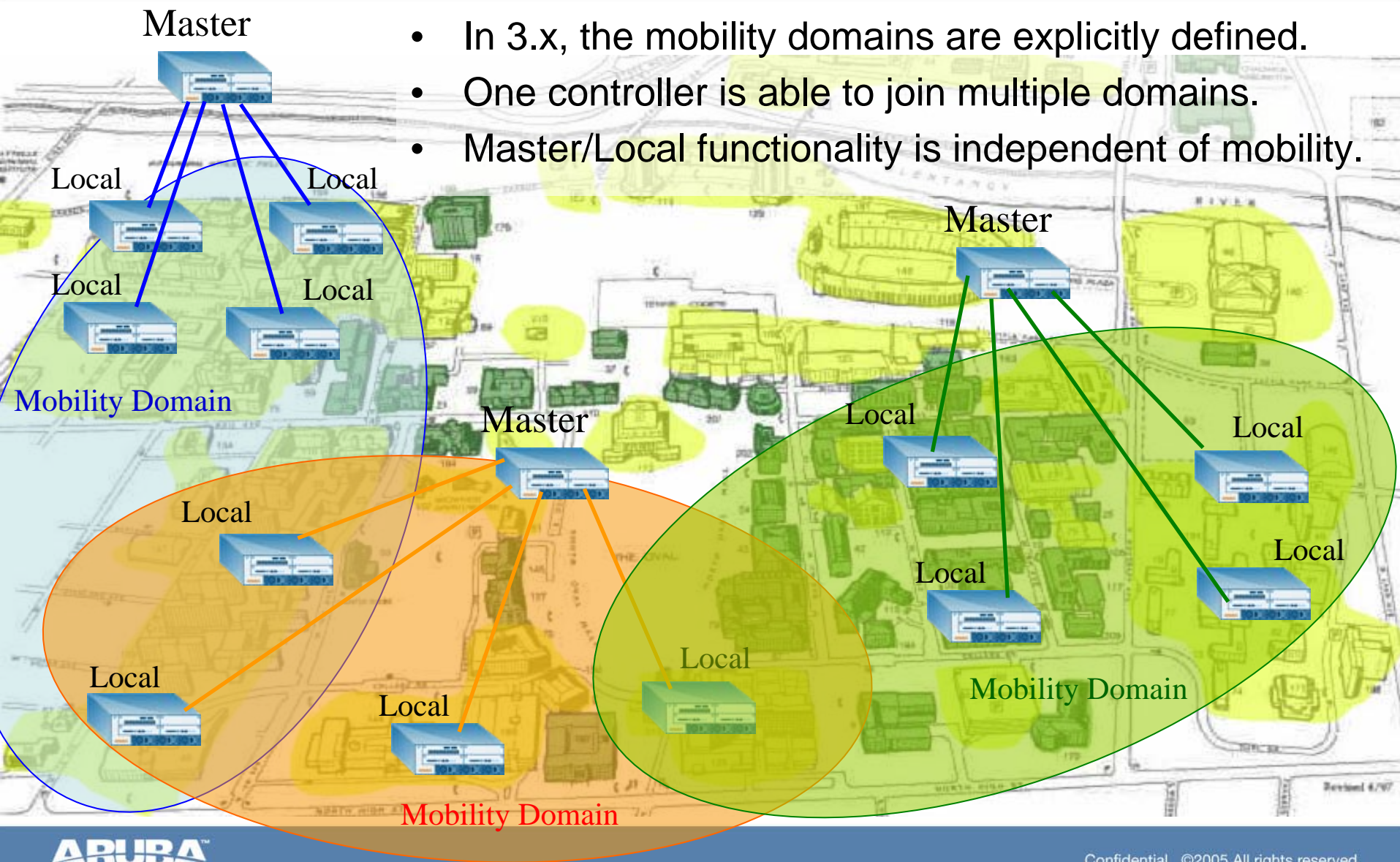
In 2.x, an area of mobility was automatically defined with a Master/Local relationship. Movement outside of one master meant a new IP



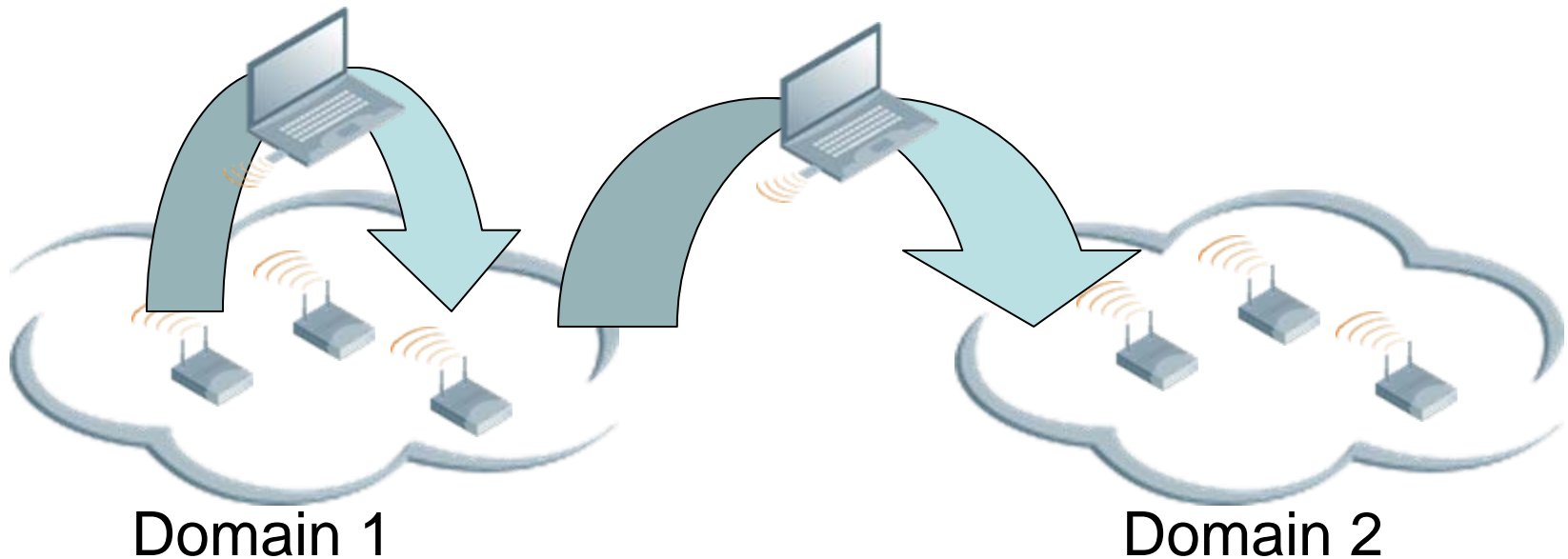


Deploying Mobility Over Large Areas

AOS 3.x



Domains Illustrated



Roaming within domain allows user to keep IP addresses, authentication, etc

When roaming between domains, the user is seen as a new user and gets a new IP, must reauthenticate, etc.

Enabling Inter-Controller L3 Mobility

Advanced Services > IP Mobility > Mobility Domain

Enable L3 Mobility

Mobility Domain Global Parameters

IP Mobility Configuration

Enable IP Mobility ☒

Mobility Domain Name Building1 Add

Domain Name	Active Domain	No of Subnets	No. of Home Agent Entry	Actions
default	Yes	0	0	Delete

Create new Mobility Domain (optional)

Apply

Configuration Updated Successfully

Commands router mobile Hide Commands

Configure Mobility Domain

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Save Configuration Logout

Network
Controller
VLANs
Ports
IP

Security
Authentication
Access Control

Wireless
AP Configuration
AP Installation

Management
General
Administration
Certificates
SNMP
Logging
Clock

Advanced Services
Redundancy
IP Mobility
Wired Access
Wireless
All Profiles

Advanced Services > IP Mobility > Mobility Domain

Mobility Domain Global Parameters

☒ IP Mobility

- ☒ Binding
- ☒ Visitor
- ☒ Active HAT Table
- ☒ Domain List
 - default

IP Mobility Domain: **default**

Active ☒

Subnet	Netmask	Vlan ID	Home Agent	Action
172.16.109.0	255.255.255.0	109	10.1.19.100	Delete
172.16.209.0	255.255.255.0	209	10.1.19.101	Delete

Add

Build Home Agent Table

Apply

Commands

```
ip mobile domain "default" hat 172.16.109.0 255.255.255.0 109 10.1.19.100
ip mobile domain "default" hat 172.16.209.0 255.255.255.0 209 10.1.19.101
```

Hide Commands

MobileIP on a per-VAP basis

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Licenses will expire in 29 days Save Configuration Log

Network
Controller
VLANs
Ports
IP

Security
Authentication
Access Control

Wireless
AP Configuration
AP Installation

Management
General
Administration
Certificates
SNMP
Logging
Clock

Advanced Services
Redundancy
IP Mobility
Stateful Firewall
External Services
Wired Access
Wireless

All Profiles

Advanced Services > All Profile Management

Profiles		Profile Details	
<ul style="list-style-type: none">+ AP+ RF Management- Wireless LAN<ul style="list-style-type: none">+ SSID Profile- Virtual AP profile<ul style="list-style-type: none">+ default+ EMEA-Corp-Employee-VAP- US-Corp-Employee-VAP<ul style="list-style-type: none">+ SSID Profile Employee-SSID+ AAA Profile US-Employee-AAA+ US-Guest-VAP+ AAA Profile+ XML API Server		Virtual AP profile > US-Corp-Employee-VAP Save As F	
Virtual AP enable	<input checked="" type="checkbox"/>	Allowed band	all ▾
VLAN	109 <-- ▾	Forward mode	tunnel ▾
Deny time range	--NONE-- ▾	Mobile IP	<input checked="" type="checkbox"/>
DoS Prevention	<input type="checkbox"/>	Station Blacklisting	<input checked="" type="checkbox"/>
Blacklist Time	3600 sec	Authentication Failure Blacklist Time	3600
Fast Roaming	<input type="checkbox"/>	Strict Compliance	<input type="checkbox"/>
VLAN Mobility	<input type="checkbox"/>		

Apply View Commands

Commands

VLAN Pooling





VLAN pooling

- For larger deployments, VLAN pooling can be used to maintain small broadcast domains while easing administrator burden of managing many small user VLANs
- VLAN pooling allows an administrator to assign a “pool” of VLANs to a campus/building instead of assigning a VLAN per building/floor.
- A hash algorithm is used on the client MAC address to distribute the users across the pool of VLANs

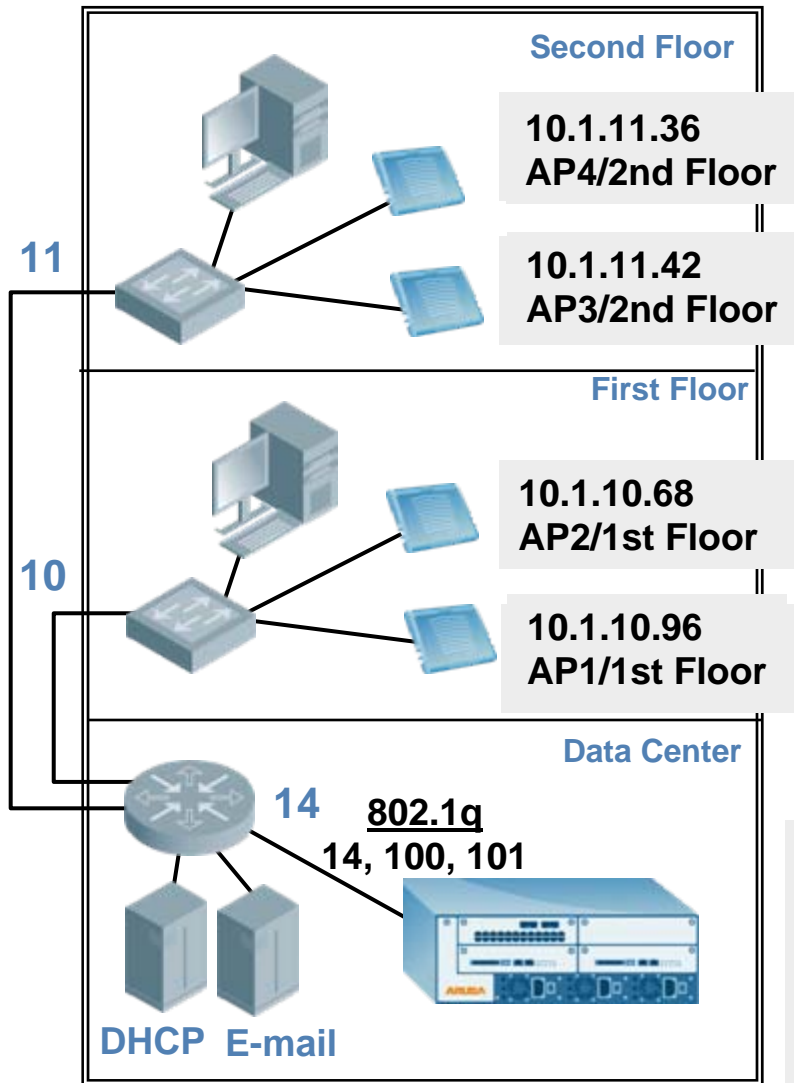
VLAN pooling cont.

- Configuration simply means assigning a range of VLANs to a Virtual AP
- Pool can be a comma-delimited list or range (or combination)
- Standard per-SSID-per-Group rules apply, simply replace single VLAN ID's with pool

The screenshot displays the Aruba Configuration Utility interface. The top navigation bar includes tabs for Monitoring, Configuration, Diagnostics, Maintenance, Plan, Events, Reports, Save Configuration, and Logout. The left sidebar shows a tree view with categories: Network (Controller, VLANs, Ports, IP), Security (Authentication, Access Control), and Wireless (AP Configuration). The main content area is titled 'Configuration > AP Group > Edit "Building2"'. It features two panels: 'Profiles' and 'Profile Details'. The 'Profiles' panel lists 'Wireless LAN', 'Virtual AP' (expanded to show 'T9-corp-Bldg2'), 'SSID Profile' (T9-corp-SSID), and 'AAA Profile' (T9-corp-AAA). The 'Profile Details' panel is titled 'Virtual AP > T9-corp-Bldg2' and contains a 'Save As' button. It has a table with two rows: 'Virtual AP' (checked) and 'VLAN' (containing the text '11-15,17'). The 'VLAN' row is highlighted with a red box. To the right of the table are fields for 'Allowed band' (set to 'all') and 'Forward mode' (set to 'tunnel').

Profiles		Profile Details	
<input type="checkbox"/> Wireless LAN		Virtual AP > T9-corp-Bldg2 Save As	
<input type="checkbox"/> Virtual AP			
<input type="checkbox"/> T9-corp-Bldg2		Virtual AP	<input checked="" type="checkbox"/>
<input type="checkbox"/> SSID Profile	T9-corp-SSID	VLAN	11-15,17
<input type="checkbox"/> AAA Profile	T9-corp-AAA		

VLAN Pooling



150-200 Users per VLAN

VLAN 101

&

VLAN 100

Layer 3 Switch

vlan 100: 10.1.100.1/24

vlan 101: 10.1.101.1/24

Mobility Controller

vlan 14: 10.1.14.6/24

loopback: 10.1.14.7/32

vlan 100: 10.1.100.6/24

vlan 101: 10.1.101.6/24

ap group "1st Floor"
vlan 100
ap group "2nd Floor"
vlan 101

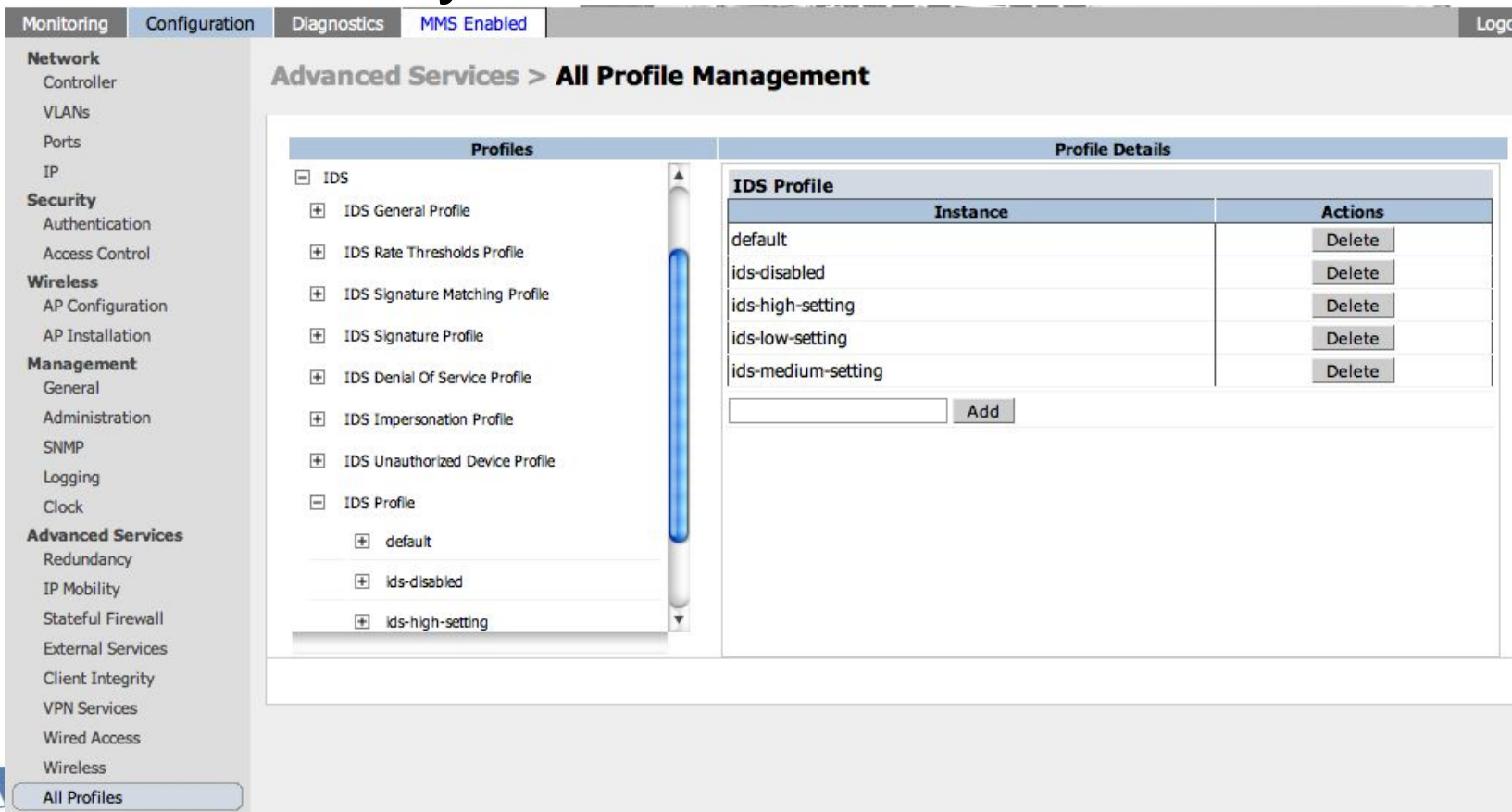
IDS



ARUBATM
The **Mobile Edge** Company

IDS Profiles

- IDS settings are now in profiles
- A set of default profiles have been created at a variety of levels



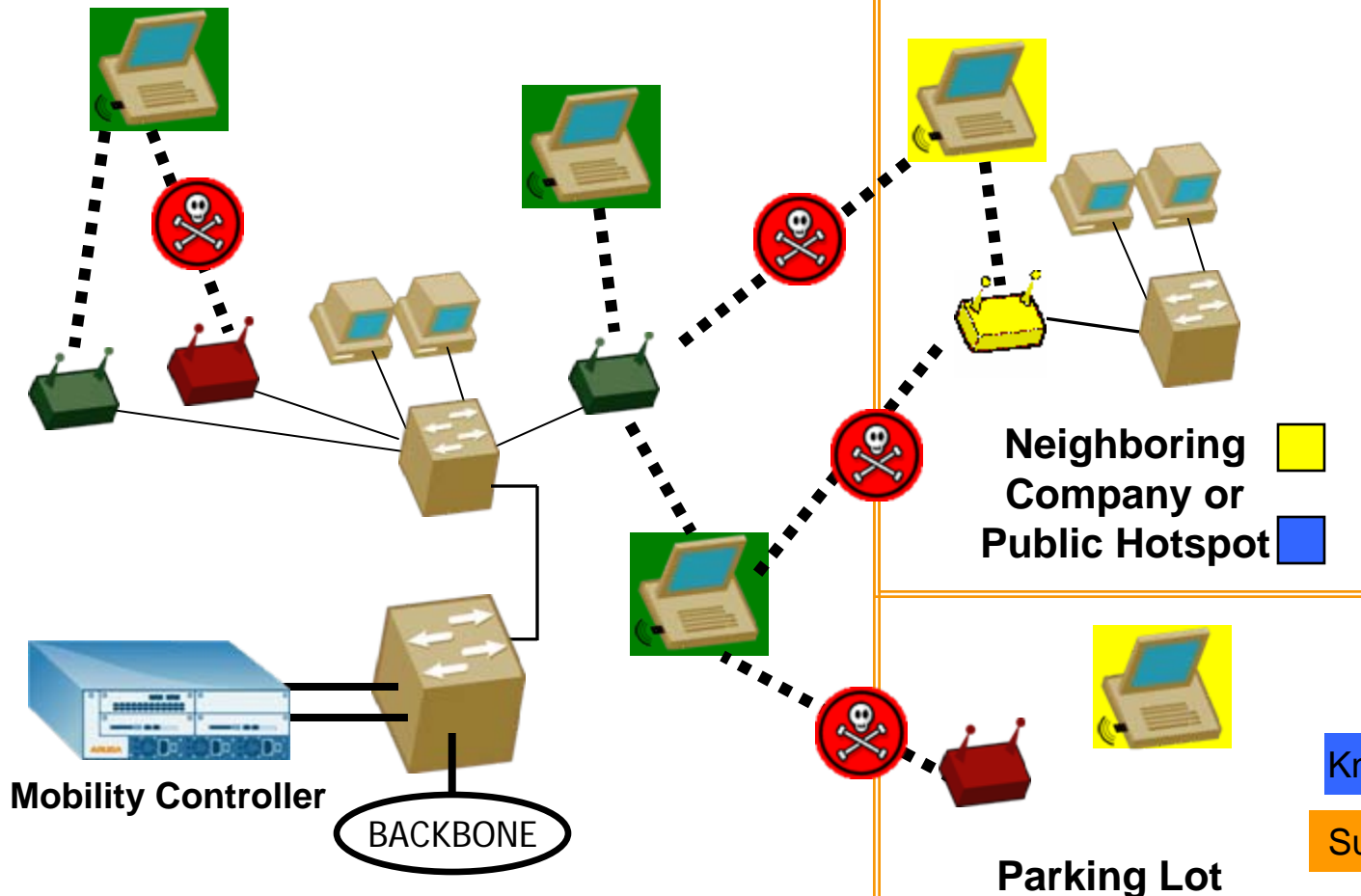
The screenshot shows a web-based configuration interface for IDS profiles. The top navigation bar includes tabs for Monitoring, Configuration, Diagnostics, and MMS Enabled. The left sidebar contains a tree view with categories: Network, Security, Wireless, and Management. Under Advanced Services, the 'All Profiles' link is selected. The main content area is titled 'Advanced Services > All Profile Management'. It features a 'Profiles' list on the left and a 'Profile Details' section on the right. The 'Profiles' list shows a hierarchy where 'IDS Profile' is expanded, revealing 'default', 'ids-disabled', and 'ids-high-setting'. The 'Profile Details' section shows a table of these profiles with 'Instance' and 'Actions' columns. Each instance has a 'Delete' button. An 'Add' button is located below the table.

Profiles	
[-] IDS	
[+] IDS General Profile	
[+] IDS Rate Thresholds Profile	
[+] IDS Signature Matching Profile	
[+] IDS Signature Profile	
[+] IDS Denial Of Service Profile	
[+] IDS Impersonation Profile	
[+] IDS Unauthorized Device Profile	
[-] IDS Profile	
[+] default	
[+] ids-disabled	
[+] ids-high-setting	

Profile Details	
IDS Profile	
Instance	Actions
default	Delete
ids-disabled	Delete
ids-high-setting	Delete
ids-low-setting	Delete
ids-medium-setting	Delete
<input type="text"/> Add	

Classification

Corporation with Aruba WIP



Rogue AP Configuration

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Licenses will expire in 30 days Save Configuration Logout

Configuration > AP Group > Edit "Building 2"

Network
Controller
VLANs
Ports
IP

Security
Authentication
Access Control

Wireless
AP Configuration
AP Installation

Management
General
Administration
Certificates
SNMP
Logging
Clock

Advanced Services
Redundancy
IP Mobility
Stateful Firewall
Wired Access
Wireless
All Profiles

Profiles

- Wireless LAN
- RF Management
- AP
- QOS
- IDS
 - IDS profile lds-low-setting
 - IDS General profile default
 - IDS Signature Matching profile factory-default-signatures
 - IDS DOS profile lds-dos-low-setting
 - IDS Impersonation profile default
 - IDS Unauthorized Device profile default**

Profile Details

IDS Unauthorized Device profile > default Save As R

Detect Adhoc Networks	<input checked="" type="checkbox"/>	Protect from Adhoc Networks	<input type="checkbox"/>
Detect Windows Bridge	<input checked="" type="checkbox"/>	Detect Wireless Bridge	<input checked="" type="checkbox"/>
Detect Devices with an Invalid MAC OUI	<input type="checkbox"/>	MAC OUI detection Quiet Time	900 sec
Adhoc Network detection Quiet Time	900 sec	Wireless Bridge detection Quiet Time	900 sec
Rogue AP Classification	<input checked="" type="checkbox"/>	Overlay Rogue AP Classification	<input checked="" type="checkbox"/>
Valid Wired MACs	<input type="checkbox"/> Delete	Rogue Containment	<input type="checkbox"/>

Apply View Commands

Commands

Enable Air Monitor

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Licenses will expire in 30 days Save Configuration Logout

Network
Controller
VLANs
Ports
IP

Security
Authentication
Access Control

Wireless
AP Configuration
AP Installation

Management
General
Administration
Certificates
SNMP
Logging
Clock

Advanced Services
Redundancy
IP Mobility
Stateful Firewall
Wired Access
Wireless
All Profiles

Configuration > AP Group > Edit "Air Monitors"

Profiles		Profile Details	
Wireless LAN		802.11g radio profile > AM Profile Save As Reset	
<input type="checkbox"/> RF Management			
<input type="checkbox"/> 802.11a radio profile	AM profile		
Adaptive Radio Management (ARM) Profile	default		
<input type="checkbox"/> 802.11g radio profile	AM Profile		
Adaptive Radio Management (ARM) Profile	default		
RF Optimization profile	default		
RF Event Thresholds profile	default		
<input type="checkbox"/> AP			
<input type="checkbox"/> QOS			
<input type="checkbox"/> IDS			

802.11g radio profile > AM Profile	
Radio enable	<input checked="" type="checkbox"/>
Channel	
Transmit Power	14
Enable CSA	<input type="checkbox"/>
Mode	am-mode
Beacon Period	100 msec
Advertise 802.11h Capability	<input type="checkbox"/>
CSA Count	4

Apply

Troubleshooting and Management Enhancements



ARUBATM
The **Mobile Edge** Company

- RF Trouble Shooting
 - Amazing tools for AP and Device debugging
 - Antenna Profile – Tells you which antenna transmits/receives better
 - Link profile – Tells you what rates are best for a given client at a given distance
 - Raw profile – General connectivity test – use it like “ping”
- Syslog API



Antenna Profile Test

- This tests if an antenna on an AP is not connected properly or if it is malfunctioning. Packets are sent to a specific target from both antennas and the difference in the received signal strength is measured. User can specify a target station or let RFT choose a random station. If the AP has only 1 antenna, then only the signal strength is displayed, no conclusion can be derived.



Antenna Profile Example

```
(Aruba5000-MX25) #rft test profile antenna-connectivity ip-addr  
172.16.25.251 dest-mac 00:16:ce:73:b5:37 radio 0
```

Transaction ID: 301

```
(Aruba5000-MX25) #show rft result all
```

```
Profile AntennaConnectivity, TransID 201, AP 172.16.25.251, Dest  
00:16:ce:73:b5:37, Radio 1
```

Antenna Connectivity Test Result

Antenna 1: Avg S/N ratio: 54	Success Rate: 99%
Antenna 2: Avg S/N ratio: 52	Success Rate: 100%
Difference: 2	1%



Link Profile Test

- This test determines the most suitable data rate for a given target. Packets are sent at different rates to find the optimal rate.



Link Profile Example

```
rft test profile link-quality ip-addr 172.16.25.251 dest-mac 00:16:ce:73:b5:37 radio 1
```

```
Show rft result all
```

```
(Aruba5000-MX25) #rft test profile link-quality ip-addr 172.16.25.251 dest-mac 00:16:ce:73:b5:37  
radio 1
```

```
Transaction ID: 4201
```

```
(Aruba5000-MX25) #show rft result all
```

```
Profile LinkQuality, TransID 4201, AP 172.16.25.251, Dest 00:16:ce:73:b5:37, Radio 1, Num Packets  
100
```

```
-----  
Data Rate  Success Rate
```

```
-----  
1.0 Mbps  100%  
2.0 Mbps  100%  
5.5 Mbps  99%  
6.0 Mbps  98%  
9.0 Mbps  100%  
11.0 Mbps 99%  
12.0 Mbps 100%  
18.0 Mbps 100%  
24.0 Mbps 100%  
36.0 Mbps 100%  
48.0 Mbps 100%  
54.0 Mbps 100%
```



Raw Profile Test

- This test is effectively a Layer 2 ping.
- A fixed number of null data packets are sent to a target and the result of the test is displayed to the user
- By default, 100 null data packets are used to test.



Raw Profile Example

(Aruba5000-MX25) #rft test profile raw ip-addr 172.16.25.251 dest-mac
00:16:ce:73:b5:37 radio 1

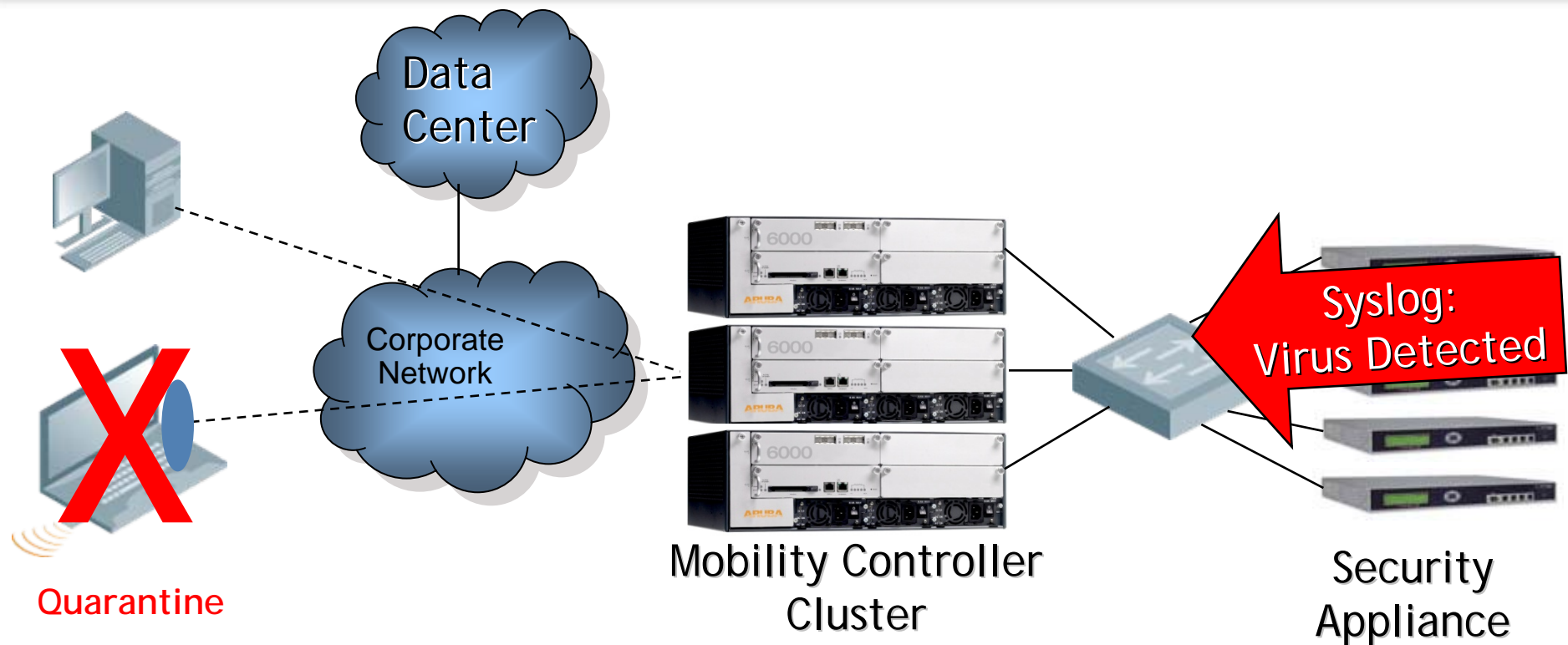
Transaction ID: 5701

(Aruba5000-MX25) #show rft result all

Profile RAW, TransID 5701, AP 172.16.25.251, Dest 00:16:ce:73:b5:37, Radio 1

```
-----  
Measurement      Value  
-----  
Total Packets    100  
Tx Success       99  
Tx Failure       1  
Excessive Retries 0  
Total Retries    1  
Avg S/N ratio    54  
Tx by Antenna 1  44  
Tx by Antenna 2  56
```

Syslog Processor



- Integrate any security or network appliance into the Mobile Edge Architecture
- Quarantine, change role, or blacklist clients based on external processing